Teoria dos Modelos
e a
Conjectura de Mordell–Lang

Vinicius Cifú Lopes

Tese apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do grau
de
Mestre em Matemática

Área de Concentração: **Matemática**
Orientador: **Prof. Dr. Francisco Miraglia Neto**
Apoio: **FAPESP** — bolsa de mestrado com reserva técnica

São Paulo — agosto — 2005

Teoria dos Modelos
e a
Conjectura de Mordell–Lang

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Vinicius Cifú Lopes e aprovada pela comissão julgadora.

São Paulo, Agosto de 2005

Banca examinadora:

- Prof. Dr. Francisco Miraglia Neto (Orientador) — IME-USP
- Prof. Dr. Ricardo Bianconi — IME-USP
- Prof. Dr. Marcelo Esteban Coniglio — CLE-UNICAMP

Teoria dos Modelos
e a
Conjectura de Mordell–Lang

Vinicius Cifú Lopes
Orientador: Prof. Dr. Francisco Miraglia
Instituto de Matemática e Estatística
Universidade de São Paulo
Apoio: FAPESP

Agosto de 2005

Apresentação

A Geometria Diofantina, cujo objetivo maior é estudar soluções inteiras de sistemas de equações polinomiais, é um dos ramos mais antigos da Matemática. As técnicas e raciocínios que utiliza transformaram-se em dois milênios e atualmente provêm, em parte, da Geometria Algébrica — teoria considerada por muitos como o topo unificador da Matemática e que já conta mais de um século.

Por outro lado, a Teoria dos Modelos tem toda a sua história nos últimos noventa anos, com origem em considerações sobre questões da Lógica Matemática que exploram as relações entre teorias e seus modelos. Os estudos da geometria interna aos modelos e dos espaços de tipos, que motivam a Estabilidade, iniciaram uma torrente de contribuições originais a todos os ramos da Matemática, em particular à Geometria Diofantina.

A Lógica moderna já contribuíra à Teoria dos Números em 1970, por exemplo, quando Matiyasevich resolveu negativamente o 10º problema de Hilbert.

Um outro problema "diofantino" clássico, a Conjectura de Mordell–Lang, foi satisfatoriamente resolvido por meios próprios da Geometria Algébrica. Trata, essencialmente, da finitude de um conjunto de soluções: "Sejam S uma variedade semi-abeliana definida sobre um corpo de característica 0, X uma subvariedade de S e Γ um grupo de divisão de um subgrupo finitamente gerado de S. Então $X \cap \Gamma$ é uma união finita de transladados de subgrupos de S." Nenhuma nova solução, baseada apenas em truques lógicos, seria de interesse. Mas conceitos como variedades algébricas e sua dimensão têm correspondentes adequados em Teoria dos Modelos, a Conjectura de Mordell–Lang equivale ela mesma a um enunciado de Estabilidade e, como Ehud Hrushovski concluiu em 1996, pode ser provada de modo uniforme e mais abrangente na nova teoria, com métodos úteis a próximos desafios. Cumpre notar que, em característica positiva, trata-se de um resultado inédito.

Esta dissertação estuda a nova abordagem.

Dividimos o texto em duas partes. A primeira introduz um subconjunto suficiente da Teoria dos Modelos para esse estudo. Entretanto, não apresentamos outros temas da teoria, de que apenas citamos alguns: omissão de tipos, estruturas o-minimais, seqüências de indiscerníveis, ultrapodutos, *back-and-forth* e a teoria geral de Estabilidade.

O capítulo introdutório apresenta uma formulação da Teoria dos Modelos que não é necessariamente a mais simples, mas sim versátil. Desse modo, não nos furtamos a definir fórmulas e estruturas e fundar todo o resto nessa escolha "clássica" e algébrica. Embora freqüentemente artigos sumarizem a teoria em termos mais abstratos e geométricos, destacando conjuntos definíveis como elementos básicos, tal forma "moderna" ainda não é suficientemente presente nos livros-texto a que se recorre muitas vezes, seja para este estudo em particular ou por motivos genéricos. Em outras palavras, a linguagem "clássica" é ainda universal, porque também sustenta a "moderna".

Também no primeiro capítulo, tomamos contato com o exemplo que nos acompanhará por todo o texto: a teoria ACF dos corpos algebricamente fechados. Contrariamente a outras classes específicas de corpos, sobre as quais toda a teoria será concentrada em um capítulo específico, essa é familiar à formação básica de todo matemático: optamos então por destacar seus atributos modelo-teóricos ao longo do texto, concomitantemente às definições genéricas que satisfaz. Além disso, não perdemos a oportunidade de comentar outras linguagens de categorias da Álgebra.

Finalmente, esse capítulo apresenta os conjuntos definíveis e suas álgebras de Boole, e os tipos como conjuntos de fórmulas ou pontos dos espaços de Stone dessas álgebras. Destacamos as relações entre esses objetos e a topologia adequada aos espaços de tipos, porque é importante familiarizar-se com tais conceitos. Concluímos com a construção do chamado "modelo monstro", uma entidade tratada de modo folclórico na literatura, mas difícil de encontrar explicitamente. Trata-se de uma estrutura com excelentes propriedades, resumidas em saturação (realização de tipos) e homogeneidade forte (existência de automorfismos) em um cardinal pré-estabelecido, mas arbitrário.

Damos grande destaque a raciocínios envolvendo a adição de constantes a linguagens — uma técnica simples e onipresente de que desejamos impregnar o leitor. Por outro lado, omitimos as demonstrações de alguns resultados que podem ser encontradas facilmente, por exemplo os Teoremas da Compacidade e de Löwenheim–Skolem e a eliminação de quantificadores de ACF. (Além das referências que indicamos, aproximadamente compatíveis com nossa exposição, incentivamos o leitor a procurar outras suas favoritas.) A Compacidade, em particular, é melhor apreciada quando usada em vez de demonstrada: são muitos os argumentos, na literatura, que dizem apenas "por compacidade" e referem-se ou à saturação de uma estrutura ou ao próprio teorema, com diversas conseqüências que demonstramos. Podemos dizer que a Compacidade, principal motor da Teoria dos Modelos, desempenha um papel análogo (e mais vital) ao do Teorema de Hahn–Banach em Análise Funcional.

Optamos por apresentar o posto de Morley bastante precocemente, no segundo capítulo, porque se faz presente em toda a exposição posterior, enquanto por si só não tem pré-requesitos. Assim, agrupamos futuramente cada definição com o estudo pertinente do posto — exceção sendo os definíveis fortemente minimais, já definidos no Capítulo 1, com breve caracterização pelo posto. Seguimos a corrente moderna que define primeiramente o posto e o grau de Morley de conjuntos definíveis e associa o posto e o grau de tipos por algumas equações versáteis; depois explicamos brevemente como entender o posto topologicamente nos espaços de tipos.

Esse capítulo segue um roteiro simples para o estudo da Estabilidade e omite algumas demonstrações que não se relacionam às técnicas que desenvolvemos. Com a meta de brevidade, também adotamos uma linha secundária na apresentação dos conceitos de deviação (*forking*) e independência e tipos definíveis e herdeiros, baseada em posto e carregada de "lemas técnicos", mas suficiente aos nossos propósitos. Entretanto, apresentamos no próprio texto referências para outras abordagens.

O Capítulo 3 estuda principalmente o importante fecho algébrico $\mathrm{acl}(\cdot)$, uma generalização do fecho homônimo de corpos. Embora o fecho em si possa ser definido e estudado já no primeiro capítulo, considerações mais sofisticadas envolvem o posto de tipos de Morley, comparando-o com a noção de dimensão que surge geometricamente. As noções de independência via posto e via fecho são identificadas. O conhecimento dos conjuntos definíveis é novamente enriquecido com o conceito de ortogonalidade.

O próximo capítulo apresenta o mais importante conceito, a nosso ver, do texto e de toda a Teoria dos Modelos: a interpretação. Mais uma vez, optamos por isolá-lo em um capítulo específico e estudar suas propriedades, embora só requeira para sua definição o conhecimento básico do Capítulo 1. Esse é o contexto adequado para enunciarmos a Conjectura de Zilber, que afirma que os corpos algebricamente fechados já respondem pela maioria das interpretações. Acrescenta-se à noção de interpretação a construção geral "eq", que permite parafrasear a noção geométrica de "modularidade local" do capítulo anterior em termos inerentes à Estabilidade.

A primeira parte encerra-se com o estudo dos grupos totalmente transcendentais. Consideramos apenas esse caso específico dos grupos estáveis, um dos desenvolvimentos mais surpreendentes da Estabilidade, porque o tratamento e o uso fundamentam-se sobre o posto ordinal. Desse modo, organizamos a seqüência de demonstrações e seu conteúdo de um modo levemente distinto da tradicional.

Apresentar a Conjectura de Mordell–Lang e sua demonstração modelo-teórica é o objetivo da segunda parte. Sua estruturação é bastante diferente: embora seu primeiro capítulo também se concentre em definições e resultados importantes, restringe-se às categorias relacionadas à conjectura. Os dois capítulos seguintes desenvolvem o maquinário necessário à demonstração e podem ser omitidos em uma primeira leitura para que se proceda imediatamente à discussão da conjectura, no quarto e último capítulo.

A primeira seção desse primeiro capítulo apresenta as novas definições com que trabalharemos e seu exemplo mais importante: a topologia de Zariski. Neste momento, os corpos algebricamente fechados, que nos acompanharam por todo o texto, mostram sua importância: o *Nullstellensatz* de Hilbert é essencialmente análogo à modelo-completude; o Teorema de Tarski–Chevalley é essencialmente análogo à eliminação de quantificadores. A segunda seção é um resumo de Geometria Algébrica no que concerne a definição de variedades, corpos de funções e dimensões entre outros, sendo brevíssimo em alguns momentos. A terceira seção apresenta alguns resultados necessários e a quarta relaciona esse material ao de Teoria dos Modelos, comparando novamente definibilidade e dimensão e posto de Morley.

O próximo capítulo analisa o artigo de Hrushovski e Zilber que introduz uma importante classe para a qual é verdadeira a Conjectura de Zilber. Esse artigo merece uma dissertação específica por sua importância intrínseca; aqui, limitamo-nos a apresentar um roteiro para sua leitura e contrastar seus pré-requesitos com nosso estudo, para adotarmos seus resultados.

Os corpos diferencialmente fechados e separavelmente fechados, tão importantes na teoria geral e para nós quanto os algebricamente fechados, são aqui definidos e estudados em bloco. De fato, selecionamos apenas os resultados necessários e referimo-nos a outros textos para demonstrações e detalhes. Por isso, optamos por inserir este capítulo como pré-requesito em vez de agrupá-lo na primeira parte e novamente sugerimos que ambas as classes sejam estudadas em dissertações próprias.

Finalmente, o último capítulo apresenta as diferentes versões da Conjectura de Mordell–Lang — para esta primeira seção, os dois capítulos anteriores não são necessários —, inclusive a equivalência com um enunciado modelo-teórico. Não poderíamos concluir de outro modo que demonstrando a conjectura por meio de todo o material desenvolvido.

O pequeno número de referências bibligráficas permite-nos identificá-las com o sobrenome do autor por extenso, seguido de algum rótulo adicional se necessário. Entendemos que, desse modo, associamos a referência ao autor (em vez de um punhado de letras) e facilitamos sua identificação visual. Sugestões de textos básicos em cada assunto são apresentadas simultaneamente à introdução do assunto.

A referência que foge a todas as regras acima é [MTAG]. Essas notas, que guiaram a redação desta dissertação, são o produto escrito de um seminário realizado em Manchester em 1994 para expor e contextualizar o trabalho de Hrushovski. Durante o processo de redação, porém, distanciamo-nos esteticamente e tecnicamente de [MTAG], preservando apenas trechos que se adaptavam à nossa apresentação. Por exemplo, não adotamos a construção de [Ziegler] de um modelo monstro constituído de classes próprias, e em geral trabalhamos em uma estrutura qualquer, não necessariamente grande.

Adotamos resultados e raciocínios de [Chang, Keisler], [Hodges] e [Poizat 1], entre outros, a quem creditaremos algumas "inspirações". Em algumas ocasiões, apoiamo-nos consideravelmente em [Marker], que também desenvolve o conteúdo de [MTAG].

Tal mesclagem possibilitou pequenas inovações em demonstrações e especialmente na ordenação do material.

Infelizmente, na guerra entre lemas técnicos e exemplos sofisticados, estes perderam uma batalha neste texto. Além de culpar a urgência da redação da dissertação, também explicamos que boa parte de seu conteúdo era novo ao autor, até mesmo as seções de tipos e modelo monstro do primeiro capítulo. Na ânsia de certificarmo-nos da corretude do que expunhamos, restringimo-nos aos exemplos necessários para a conclusão do estudo.

Mesmo antes ou fora do curso de Mestrado, muitos contribuíram para o progresso do autor e desta redação. Preferimos recordá-los de modo exato ao discorrer imprecisamente aqui; a todos o nosso agradecimento. Destacamos apenas, dentre essas contribuições, a orientação do Prof. Francisco Miraglia, a participação ativa dos Profs. Ricardo Bianconi, Marcelo Esteban Coniglio e Marcelo Finger em nossas bancas de defesa e qualificação, e o apoio da FAPESP na forma de bolsa de mestrado com reserva técnica.

Introduzimos agora informações úteis por todo o texto:

Pré-requesitos

Na Teoria dos Modelos, faz-se mais uso da Teoria dos Conjuntos moderna que em outras áreas da Matemática. Isso torna necessário fixar alguma teoria dos conjuntos: trabalharemos com ZFC, a Teoria dos Conjuntos de Zermelo–Fraenkel com o Axioma da Escolha, e as definições usuais de n-uplas ordenadas, relações, ordinais e cardinais, entre outras. Mais precisamente, elegemos o Apêndice A de [Chang, Keisler] como o material adequado, de modo que nossa teoria dos conjuntos corresponde àquela usualmente vista nos cursos de graduação. O Capítulo 8 de [Poizat 1] e o Apêndice A de [Marker] também são bastante informativos.

Também usaremos recursos de Álgebras de Boole. Em geral, as definições e resultados necessários já se encontram nos livros de Teoria dos Modelos: a Seção 6.2 de [Hodges] ou, em [Chang, Keisler], os Exemplo 1.4.3 e Proposição 4.1.1 e os comentários que os seguem, além do Exercício 1.4.9. O leitor deve atentar especificamente para os conjuntos "com a propriedade de intersecção finita", "filtro (próprio)" e "ultrafiltro", todos não-vazios, e que cada um estende-se ao próximo pelo Lema de Zorn. Estas formulações equivalentes do conceito de ultrafiltro serão de uso freqüente: (i) filtro próprio maximal; (ii) filtro a que um elemento pertence se e somente se seu complemento não; (iii) filtro próprio ("primo") que, contendo a união de dois elementos, contém ao menos um deles. Ao considerar os conjuntos de tipos como espaços de Stone, detalharemos as propriedades necessárias.

Uma combinação booleana é finita, ou seja, obtida por um número finito de operações sucessivas de união, intersecção e complementação sobre os conjuntos originais, ou de disjunção, conjunção e negação no caso de fórmulas.

Ao fazermos recurso avançado a tópicos de Topologia ou Álgebra, apresentaremos localmente os conceitos e as referências apropriadas, bastando para a leitura os conhecimentos dos currículos de graduação.

Notações e convenções

Os símbolos $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ denotam respectivamente os conjuntos de números naturais, inteiros, racionais, reais e complexos, considerados cada um como a extensão natural dos anteriores. Esses símbolos também representarão as estruturas algébricas e de ordem usuais com tais domínios. Incluímos o zero em $\mathbb{N}$, de modo que $\mathbb{N}$ e ω são precisamente o mesmo conjunto. O símbolo *, aplicado a qualquer desses conjuntos ou a um corpo, representa tal conjunto sem o zero, ou seja, $\mathbb{N}^* = \mathbb{N} - \{0\}$.

O sinal $+$ pode denotar soma cardinal ou ordinal — o sucessor do ordinal ξ é $\xi + 1$. Por definição, 0 é um ordinal limite, mas trataremos esse caso separadamente; referimo-nos sempre a ordinais limites não-nulos. O menor cardinal infinito é ω e os cardinais usualmente indicados $\aleph_\xi$ serão escritos ω_ξ. O sucessor do cardinal α é α^+, de modo que $(\omega_\xi)^+ = \omega_{\xi+1}$. A cardinalidade de um conjunto X é indicada $|X|$.

De modo a trabalhar com os postos que definiremos, introduzimos dois símbolos -1 e ∞, que deverão ser interpretados respectivamente como "menor" e "maior" que todos os ordinais, ou seja, $-1 < \xi < \infty$ para qualquer ordinal ξ. O supremo de uma classe de ordinais é definido como ∞ se for ilimitada e -1 se for vazia. Como -1 e ∞ são apenas símbolos, essas interpretações podem ser formalizadas em ZFC.

Letras não identificadas representam números naturais, de modo que expressões como $m \geqslant 1$ e $r \geqslant s$ têm seu significado usual, ou seja, $m \in \mathbb{N}^*$ e $s \leqslant r < \omega$, e indexações $x_1, \ldots, x_n$ são finitas de 1 a n, podendo ser vazias com $n = 0$. Esta regra, porém, tem muitas exceções. Conjuntos de fórmulas, por exemplo, são sempre não-vazios (veja pág. 15), assim como $n \neq 0$ quando se *tomam* $D_1, \ldots, D_n \in D$ ou considera-se X^n.

Índices ordinais transfinitos e elementos de conjuntos-índice gerais serão devidamente apresentados.

O conjunto das funções de X a Y é indicado Y^X. Se $f \in Y^X$ e $(x_i)_{i \in I}$ é uma seqüência em X, é conveniente definir $f((x_i)_{i \in I}) = (f(x_i))_{i \in I}$.

Escrever por extenso seqüências de variáveis $v_1, \ldots, v_m$ e n-uplas $(a_1, \ldots, a_n)$ de elementos de um domínio freqüentemente transtorna a manipulação de fórmulas. Convenciona-se, então, escrever apenas uma letra, sendo o comprimento da seqüência determinado pelo contexto; assume-se que as variáveis são distintas, enquanto que os elementos da n-upla podem não ser. Por exemplo, $\exists v\, \phi(v, a)$ abrevia $\exists v_1 \ldots \exists v_m\, \phi(v_1, \ldots, v_m, a_1, \ldots, a_n)$. Em enunciados e definições, explicitaremos tal "contexto". Se u, v são seqüências de n variáveis, digamos $u_1, \ldots, u_n$ e $v_1, \ldots, v_n$ respectivamente, $u = v$ abrevia realmente $((u_1 = v_1) \wedge \ldots \wedge (u_n = v_n))$.

A n-upla $a = (a_1, \ldots, a_n)$ pode representar também o conjunto $a = \{a_1, \ldots, a_n\}$. Isso é especialmente útil na descrição de conjuntos de parâmetros: XYa abrevia $X \cup Y \cup \{a_1, \ldots, a_n\}$. Se também $b = (b_1, \ldots, b_k)$, então ab é a seqüência $(a_1, \ldots, a_n, b_1, \ldots, b_k)$, que podemos indicar também (a, b), ou o conjunto $\{a_1, \ldots, a_n, b_1, \ldots, b_k\}$. Novamente, explicitaremos o contexto adequado.

Outras notações serão introduzidas no corpo do texto. Alguns símbolos estão relacionados no início do Índice.

Cuidado: textos de Teoria dos Modelos em geral escrevem "modelo M" e "conjunto de parâmetros $A \subseteq M$", sendo exceções [Chang, Keisler] e [Hodges]. Usaremos "estrutura $\mathfrak{A}$ com domínio A", sempre o domínio indicado pela letra itálica correspondente, e "conjunto de parâmetros $X \subseteq A$". Optamos pela antiga grafia para ressaltar visualmente os conjuntos que são domínios de estruturas.

Em geral, ao indicarmos $\mathfrak{A}, \mathfrak{A}_i, \mathfrak{B}, \mathfrak{C}$, assumimos que são todas estruturas adequadas para a mesma linguagem, exceções feitas na definição de interpretação e na construção "eq" e no estudo de geometrias de Zariski. Também geralmente, ao trabalhar com conjuntos de fórmulas, consideraremos uma única linguagem e as estruturas apropriadas. Um tal conjunto define a linguagem dos símbolos que ocorrem em suas fórmulas, ou seja, a menor linguagem em que pode ser escrito. Finalmente, quando se trabalha com diversas linguagens, mencionam-se seus símbolos comuns: evidentemente, assume-se que tenham também a mesma aridade e a mesma interpretação.

Usaremos o mesmo operador $\mathrm{cl}(\cdot)$, que abrevia em inglês *closure*, para o fecho combinatório em uma pré-geometria e o fecho topológico. Neste caso, a única obstrução ao uso da barra superior será o comprimento gráfico de alguns argumentos.

Invariância

Sejam $S \subseteq X^n$ e $\mathscr{F}$ um conjunto de funções de X em X, isto é, $\mathscr{F} \subseteq X^X$. Explicitamos estas definições:

(i) S é *fixado por* ou *invariante sob* $\mathscr{F}$ se $f[S] = S$ para todo $f \in \mathscr{F}$. (Em inglês, S é fixado *setwise* por $\mathscr{F}$.) No caso particular de f ser uma bijeção, a igualdade equivale a $x \in S \Leftrightarrow f(x) \in S$ para todo $x \in X^n$.

(ii) Os elementos de S são *fixados por* ou *invariantes sob* $\mathscr{F}$ se $f(x) = x$ para todos $f \in \mathscr{F}$ e $x \in S$. (Em inglês, S é fixado *pointwise* por $\mathscr{F}$.)

É preciso cuidado, porque, em muitos textos de Teoria dos Modelos ou Álgebra, por "S invariante sob f" pode-se entender $f[S] \subseteq S$ ou que os elementos de S são fixados por f.

Sumário

Teoria Geométrica dos Modelos

1

O ambiente

Descrevemos, neste capítulo, as noções básicas da Teoria dos Modelos e a obtenção do modelo monstro. Buscamos uma introdução breve: não numeramos definições e omitimos algumas demonstrações. O leitor sem experiência prévia poderá consultar [Marker] ou o heterodoxo [Poizat 1], que inclui em sua definição a estrutura vazia. Os textos homônimos [Chang, Keisler] e [Hodges] são referências abrangentes, embora o primeiro não cubra as ramificações atuais da teoria e o segundo trabalhe com linguagens infinitárias e também a estrutura vazia. Um exemplo de como a teoria pode ser compactamente introduzida em um artigo é [Bouscaren A], além dos artigos com que trabalharemos, como veremos quando introduzirmos os subconjuntos definíveis.

Construímos a teoria sucintamente, mas incluímos a formalização de termos e fórmulas. Algumas noções admitem muitas formulações equivalentes, das quais procuramos as mais simples, embora frisemos e usemos algumas caracterizações imediatas.

1.1. Introdução

Para fixar notação e recordar alguns fatos, inicialmente revisaremos o Cálculo de Predicados de primeira ordem com igualdade. Introduziremos então a Teoria dos Modelos básica e clássica, de modo adequado ao desenvolvimento posterior.

Consideremos a definição de grupo, um conceito bastante comum em Matemática. Um grupo é um conjunto (não-vazio) munido de uma operação binária que satisfaz determinadas propriedades, ditas de grupo — uma delas destaca a existência de um elemento (constante) neutro. Primeiramente, concentrar-nos-emos em isolar a "operação" e a "constante", depois em como expressar tais "propriedades" e, enfim, descrever como um "grupo" é uma estrutura adequada para usar-se tal vocabulário e porque uma tal estrutura é ou não um grupo. Poderíamos também optar por outra abordagem: introduzir estruturas imediatamente depois das linguagens.

Uma *linguagem* L constitui-se de conjuntos I, J, K e funções $\mu : I \to \mathbb{N}^*$, $\nu : J \to \mathbb{N}^*$. Fazemos corresponder um *predicado* P_i a cada $i \in I$, um *operador* f_j a cada $j \in J$, uma *constante* c_k a cada $k \in K$. Como formalizaremos a seguir, o predicado P_i é $\mu(i)$-ário (necessita $\mu(i)$ argumentos) e o operador f_j é $\nu(j)$-ário.

Adotamos como conectivos lógicos a negação $\neg$ e a conjunção $\wedge$ e como quantificador o existencial $\exists$. Dispomos de parênteses, o sinal de igualdade $=$ e uma quantidade infinita de variáveis v_n, $n \in \mathbb{N}$.

Definimos agora os *termos* de L, obtidos por aplicação finita destas regras: (i) v_n e c_k são termos, para $n \in \mathbb{N}$ e $k \in K$; (ii) se $t_1, \dots, t_{\nu(j)}$ são termos, então $f_j(t_1, \dots, t_{\nu(j)})$ é um termo, para $j \in J$.

Definimos então as *fórmulas atômicas* de L: (i) se t, t' são termos, então $t = t'$ é uma fórmula atômica; (ii) se $t_1, \dots, t_{\mu(i)}$ são termos, então $P_i(t_1, \dots, t_{\mu(i)})$ é uma fórmula atômica, para $i \in I$.

Finalmente, definimos as *fórmulas (bem-formadas)* de L, obtidas por aplicação finita destas regras: (i) fórmulas atômicas são fórmulas; (ii) se v é uma variável e ϕ, ψ são fórmulas, então $\neg\phi$, $(\phi \wedge \psi)$, $\exists v\, \phi$ são fórmulas. Removeremos ou adicionaremos parênteses às fórmulas como for conveniente; a precedência usual é $\neg$, $\exists$, $\wedge$.

Frisamos o caráter *finitário* das regras de formação de termos e fórmulas, que então têm sempre comprimento finito, fundamental para o desenvolvimento e raciocínio posteriores. Sugerimos que o leitor tenha sempre em vista esse fato.

Uma tarefa que ignoramos é assegurar a ausência de ambigüidades, por exemplo que o símbolo $\neg$ e a seqüência $\exists v$ diferem, e que a formação de uma fórmula é única. Assumimos também que os conjuntos de fórmulas, de sentenças (que definiremos a seguir) e de símbolos (I, J, K) de L foram construídos como realmente conjuntos de ZFC. Verifica-se que tais conjuntos têm a mesma cardinalidade $|L| = \max\{\omega, |I|, |J|, |K|\}$, dita o *cardinal de* L.

Em $\exists v\, \phi$, a fórmula ϕ é o *escopo* da quantificação $\exists v$ e qualquer ocorrência de v em ϕ é dita *ligada*. Uma ocorrência que não é ligada chama-se *livre*. Se $v_{i_1}, \dots, v_{i_k}$ são as variáveis que ocorrem livres em ϕ, indica-se $\phi(v_{i_1}, \dots, v_{i_k})$. Uma fórmula sem variáveis livres é chamada *sentença*. Futuramente, escreveremos $\phi(v_1, \dots, v_n)$ para indicar que as variáveis livres de ϕ são algumas ou todas dentre $v_1, \dots, v_n$. Ao ler esta seção, é um exercício verificar que tal ambigüidade não causa confusão e que o segundo modo, por ser mais geral, é mais útil.

Embora não seja necessário — as definições desta seção permaneceriam adequadas —, suporemos que, em uma fórmula, nenhuma variável ocorre simultaneamente livre e ligada e tampouco há duas quantificações aninhadas de uma mesma variável (caso em que a exterior é redundante). Isso facilita a leitura das fórmulas e simplifica algumas operações, como a substituição.

Introduzimos as abreviaturas clássicas, para ϕ, ψ fórmulas e v variável:

$(\phi \vee \psi)$ abrevia $\neg(\neg\phi \wedge \neg\psi)$ — disjunção;

$(\phi \rightarrow \psi)$ abrevia $\neg(\phi \wedge \neg\psi)$ — implicação;

$(\phi \leftrightarrow \psi)$ abrevia $((\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi))$ — equivalência;

$\forall v\, \phi$ abrevia $\neg \exists v\, \neg \phi$ — quantificação universal.

Se t, t' são termos, $t \neq t'$ abrevia $\neg(t = t')$.

Quando Φ é um conjunto *finito e não-vazio* de fórmulas, digamos $\Phi = \{\phi_1, \ldots, \phi_n\}$ com $n \geqslant 1$, então $\bigwedge \Phi$ abrevia $(\phi_1 \wedge \ldots \wedge \phi_n)$ e $\bigvee \Phi$ abrevia $(\phi_1 \vee \ldots \vee \phi_n)$. Esta é uma exceção à convenção de indexações vazias: para evitar má-formação de fórmulas (não definimos a *fórmula vazia*), obrigatoriamente $n \neq 0$. A ordem em que é feita a conjunção não é importante, porque trabalharemos com fórmulas equivalentes.

O *fecho* de uma fórmula é obtido quantificando-se *universalmente* todas as suas variáveis livres.

Uma *estrutura* ou *realização* $\mathfrak{A}$ para a qual a linguagem L é apropriada, ou L-*estrutura*, constitui-se de um *domínio* $A \neq \emptyset$ e relações $R_i^{\mathfrak{A}} \subseteq A^{\mu(i)}$, $i \in I$, funções ou operações $f_j^{\mathfrak{A}} : A^{\nu(j)} \rightarrow A$, $j \in J$, e constantes ou elementos distinguidos $c_k^{\mathfrak{A}} \in A$, $k \in K$. Cada $R_i^{\mathfrak{A}}, f_j^{\mathfrak{A}}, c_k^{\mathfrak{A}}$ é uma *interpretação* de P_i, f_j, c_k respectivamente. Escreve-se $\mathfrak{A} = (A, (R_i^{\mathfrak{A}})_{i \in I}, (f_j^{\mathfrak{A}})_{j \in J}, (c_k^{\mathfrak{A}})_{k \in K})$.

Associamos a cada variável v_n um *parâmetro* $a_n \in A$, obtendo uma *valoração* x. A valoração obtida de x substituindo-se a_n por $a \in A$ é indicada $x\binom{n}{a}$.

Devemos inicialmente calcular os termos: (i) $[v_n]_x^{\mathfrak{A}} = a_n$ e $[c_k]_x^{\mathfrak{A}} = c_k^{\mathfrak{A}}$; (ii) $[f_j(t_1, \ldots, t_{\nu(j)})]_x^{\mathfrak{A}} = f_j^{\mathfrak{A}}([t_1]_x^{\mathfrak{A}}, \ldots, [t_{\nu(j)}]_x^{\mathfrak{A}})$.

Definimos satisfação de fórmulas por indução em sua formação:

$$\begin{aligned}
\mathfrak{A} \models_x t = t' \quad &\Leftrightarrow \quad [t]_x^{\mathfrak{A}} = [t']_x^{\mathfrak{A}}\ ; \\
\mathfrak{A} \models_x P_i(t_1, \ldots, t_{\mu(i)}) \quad &\Leftrightarrow \quad ([t_1]_x^{\mathfrak{A}}, \ldots, [t_{\mu(i)}]_x^{\mathfrak{A}}) \in R_i^{\mathfrak{A}}\ ; \\
\mathfrak{A} \models_x (\phi \wedge \psi) \quad &\Leftrightarrow \quad \mathfrak{A} \models_x \phi \text{ e } \mathfrak{A} \models_x \psi\ ; \\
\mathfrak{A} \models_x \neg\phi \quad &\Leftrightarrow \quad \text{não } \mathfrak{A} \models_x \phi\ ; \\
\mathfrak{A} \models_x \exists v_n\, \phi \quad &\Leftrightarrow \quad \text{existe } a \in A \text{ tal que } \mathfrak{A} \models_{x\binom{n}{a}} \phi\,.
\end{aligned}$$

Assim, dados $\mathfrak{A}$, uma fórmula $\phi(v_{i_1}, \ldots, v_{i_k})$ e $a_{i_1}, \ldots, a_{i_k} \in A$, dizemos que com tais parâmetros ϕ é *válida* ou *satisfeita* em $\mathfrak{A}$ e $\mathfrak{A}$ *satisfaz* ou *realiza* ou *é modelo de* ϕ se $\mathfrak{A} \models_x \phi$ para uma valoração x com tais parâmetros. Vemos que isso independe dos valores de x nas outras variáveis, de modo que se escreve simplesmente $\mathfrak{A} \models \phi(a_{i_1}, \ldots, a_{i_k})$ e diz-se que $(a_{i_1}, \ldots, a_{i_k})$ *satisfaz* ou *realiza* ϕ em $\mathfrak{A}$.

Se Σ é um conjunto de sentenças de L e $\mathfrak{A} \models \sigma$ para toda $\sigma \in \Sigma$, indica-se $\mathfrak{A} \models \Sigma$. A mesma nomenclatura de satisfação aplica-se a este caso.

Suponha $\mathfrak{A}$ uma L-estrutura e X um subconjunto de seu domínio A. Adicione a L mais constantes, uma para cada elemento de X, obtendo uma linguagem $\mathrm{L}(X)$. Observe que $|\mathrm{L}(X)| = |\mathrm{L}| + |X| = \max\{|\mathrm{L}|, |X|\}$. Como em qualquer expansão de linguagens, as fórmulas e sentenças de L são ainda fórmulas e sentenças de L(X). Também $(\mathfrak{A}, (x)_{x\in X})$ é uma L(X)-estrutura, com cada $x \in X$ interpretando sua constante, usualmente também indicada x; em algumas ocasiões, não havendo ambigüidade, escreveremos apenas $\mathfrak{A}$ para não sobrecarregar. Note ainda que a definição de satisfação pode ser feita sem menção a valorações, com o expediente de considerar apenas sentenças de L(A). Enfim, quando conveniente, consideraremos fórmulas de L com parâmetros em X como fórmulas de L(X) e reciprocamente.

O domínio de uma estrutura (em letra gótica) é indicado pela letra romana correspondente. A cardinalidade de uma estrutura $\mathfrak{A}$ é simplesmente $|A|$. Abandonaremos o uso de índices superiores nas relações e operadores: por exemplo, adotaremos a representação $\mathfrak{A} = (A, (R_i)_{i\in I}, (f_j)_{j\in J}, (a_k)_{k\in K})$ e $\mathfrak{B} = (B, (S_i)_{i\in I}, (g_j)_{j\in J}, (b_k)_{k\in K})$, explicando quando necessário.

Entre estruturas $\mathfrak{A}, \mathfrak{B}$ apropriadas para uma mesma linguagem L, definem-se algumas relações que generalizam as da Álgebra cotidiana e que passamos a descrever.

$\mathfrak{A}$ é *subestrutura* de $\mathfrak{B}$ ou $\mathfrak{B}$ é *extensão* de $\mathfrak{A}$, em símbolos $\mathfrak{A} \subseteq \mathfrak{B}$, se $A \subseteq B$ e (i) as relações de $\mathfrak{A}$ são as restrições das correspondentes de $\mathfrak{B}$, isto é, $R_i = S_i|_A = S_i \cap A^{\mu(i)}$; (ii) os operadores de $\mathfrak{A}$ são as restrições dos correspondentes de $\mathfrak{B}$, isto é, $f_j = g_j|_A$; (iii) as constantes de $\mathfrak{A}$ são as correspondentes de $\mathfrak{B}$, isto é, $a_k = b_k$. Note que, então, é necessário $g_j[A^{\nu(j)}] \subseteq A$ para cada $j \in J$ e $b_k \in A$ para cada $k \in K$.

Uma *imersão* $h : \mathfrak{A} \to \mathfrak{B}$ é uma injeção $h : A \to B$ que transporta $\mathfrak{A}$ a uma subestrutura de $\mathfrak{B}$, deste modo: $(a_1, \ldots, a_{\mu(i)}) \in R_i \Leftrightarrow (h(a_1), \ldots, h(a_{\mu(i)})) \in S_i$ (a igualdade também é preservada, pois h é injetora); $f_j(a_1, \ldots, a_{\nu(j)}) = a \Leftrightarrow g_j(h(a_1), \ldots, h(a_{\nu(j)})) = h(a)$; $h(a_k) = b_k$.

Caso h seja também sobrejetora, é chamada *isomorfismo* e indicamos $\mathfrak{A} \cong \mathfrak{B}$. A inversa de um isomorfimo é um isomorfismo, porque a definição de imersão é feita com equivalências. Vemos também que a identidade e a composição de isomorfismos são isomorfismos. Como usual, um *automorfismo* de $\mathfrak{A}$ é um isomorfismo de $\mathfrak{A}$ a $\mathfrak{A}$ e os *automorfismos sobre* $X \subseteq A$ são os automorfismos de $\mathfrak{A}$ que fixam os elementos de X.

Uma imersão $h : \mathfrak{A} \to \mathfrak{B}$ é dita *elementar* se preservar a validade de todas as fórmulas, ou seja, $\mathfrak{A} \models \phi(a_1, \ldots, a_n) \Leftrightarrow \mathfrak{B} \models \phi(h(a_1), \ldots, h(a_n))$ para quaisquer $\phi(v_1, \ldots, v_n)$ fórmula de L e $a_1, \ldots, a_n \in A$. Considerando $\neg\phi$, vemos que bastam a implicação direta ou a inversa.

Vemos também, pela definição de satisfação, que qualquer imersão preserva a validade das fórmulas sem quantificadores (também ditas *abertas*).

Se $\mathfrak{A} \subseteq \mathfrak{B}$ e a identidade for (imersão) elementar, escreve-se $\mathfrak{A} \prec \mathfrak{B}$, pospondo-se o adjetivo "elementar" aos termos "subestrutura" e "extensão".

Observamos que um isomorfismo é uma imersão elementar, o que pode ser verificado por indução na complexidade das fórmulas.

Define-se que $\mathfrak{A}$ é *elementarmente equivalente* a $\mathfrak{B}$ e indica-se $\mathfrak{A} \equiv \mathfrak{B}$ quando, para toda sentença σ de L, $\mathfrak{A} \models \sigma \Leftrightarrow \mathfrak{B} \models \sigma$. Novamente, considerando $\neg\sigma$, vemos que basta uma das implicações.

É possível definir imersão e equivalência elementares sem recurso a fórmulas, por meio de isomorfismos locais e *back-and-forth*, como em [Hodges] (jogos) e [Poizat 1].

Agora detemos um número suficiente de conceitos para vê-los exemplificados. Começamos por observar que a condição de imersão elementar reescreve-se em termos de equivalência elementar: se $\mathfrak{A} \subseteq \mathfrak{B}$ e $X \subseteq A$, então $\mathfrak{A} \prec \mathfrak{B} \Leftrightarrow (\mathfrak{A}, (x)_{x\in X}) \prec (\mathfrak{B}, (x)_{x\in X}) \Rightarrow (\mathfrak{A}, (x)_{x\in X}) \equiv (\mathfrak{B}, (x)_{x\in X})$, valendo a implicação inversa se $X = A$. Finalmente, notamos que toda imersão elementar, inclusive isomorfismos, implica equivalência elementar.

Lidaremos principalmente com linguagens apropriadas para estruturas algébricas, que apresentaremos na próxima seção. Contudo, outras linguagens também fornecerão exemplos úteis, como a linguagem das relações de ordem, um clássico da literatura.

Exemplo 1.1.1 (Ordens). A linguagem das ordens contém um único predicado binário, indicado (assim como as relações correspondentes) pelo símbolo $\leqslant$ infixo. É usual $x < y$ abreviar $((x \leqslant y) \wedge (x \neq y))$.

Consideremos a estrutura ordenada $\mathbb{N}$. Por exemplo, $\mathbb{N} \models \exists x \forall y\, (x \leqslant y)$, porque 0 é o mínimo de $\mathbb{N}$, mas $\mathbb{N} \models \neg\exists x \forall y\, (y \leqslant x)$. Além disso, se $\phi(x, y)$ é a fórmula $\neg\exists z\, ((x < z) \wedge (z < y))$, então $\mathbb{N} \models \phi(n, n+1)$ para todo $n \in \mathbb{N}$. Suponha, agora, $\mathbb{N} \prec \mathfrak{A} = (A, \leqslant)$. Como a extensão é elementar, $\mathfrak{A} \models \phi(n, n+1)$. Vemos, do mesmo modo, que 0 é o mínimo de A e concluímos que todos os elementos de $A - \mathbb{N}$ são precedidos por todos os de $\mathbb{N}$. Raciocínios análogos (em que se possam escrever fórmulas) mostram que A é linearmente ordenado e que não tem um máximo, entre outros fatos que valem em $\mathbb{N}$. Em particular, $A - \mathbb{N}$ é infinito, porque caso contrário teria máximo.

Com suas ordens usuais, $\mathbb{Q}$ é subestrutura de $\mathbb{R}$. Mostraremos no Exemplo 1.1.5 que $\mathbb{Q} \prec \mathbb{R}$. Porém, tomando $\overline{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ com a ordem usual, vemos que $\overline{\mathbb{R}}$ não é nem mesmo elementarmente equivalente a $\mathbb{Q}$ ou $\mathbb{R}$, porque tem pontos inicial e final, ainda que $\mathbb{Q} \subseteq \mathbb{R} \subseteq \overline{\mathbb{R}}$ como estruturas.

Exemplo 1.1.2 (Igualdade). Por nossa definição, uma linguagem sem predicados, operadores ou constantes contém ainda o símbolo de igualdade $=$ (portanto, existindo fórmulas). As "estruturas" apropriadas para essa linguagem são os conjuntos (domínios puros, sem estrutura).

Vejamos agora um uso importante do símbolo de igualdade em uma linguagem L arbitrária. Seja $\phi(v)$ uma fórmula de L em que v é uma seqüência de m variáveis livres; não indicaremos outras possíveis variáveis (parâmetros) de ϕ. Suponha $k \in \mathbb{N}^*$ e $v_1, \ldots, v_k$ seqüências de m novas variáveis. Definimos

$$\exists^{\leqslant k} v\, \phi(v) : \exists v_1 \ldots \exists v_k \forall v \left(\phi(v) \to \bigvee_{i=1}^{k} (v = v_i) \right) ,$$

em que não há variáveis livres, exceto talvez outros parâmetros de ϕ. Para uma L-estrutura $\mathfrak{A}$, temos $\mathfrak{A} \models \exists^{\leqslant k} v\, \phi(v)$ se e somente se há no máximo k elementos de A^m que satisfazem ϕ ou, na notação que definiremos, $|\phi(\mathfrak{A})| \leqslant k$. Note que, em nossa formulação, pode ***não*** haver elemento que satisfaça ϕ. Definindo $\exists^{\geqslant 1} v\, \phi(v) : \exists v\, \phi(v)$ e $\exists^{\geqslant j} v\, \phi(v) : \neg \exists^{\leqslant j-1} v\, \phi(v)$ para $j \geqslant 2$, temos $\mathfrak{A} \models \exists^{\geqslant k} v\, \phi(v) \Leftrightarrow |\phi(\mathfrak{A})| \geqslant k$. Finalmente, com $\exists^{=k} v\, \phi(v) : \exists^{\leqslant k} v\, \phi(v) \wedge \exists^{\geqslant k} v\, \phi(v)$, vemos que $\mathfrak{A} \models \exists^{=k} v\, \phi(v) \Leftrightarrow |\phi(\mathfrak{A})| = k$. Deixamos a cargo do leitor escrever as fórmulas para $k = 0$.

É conseqüência do Teorema da Compacidade (Teorema 1.1.9) que não há sentença σ da linguagem de igualdade satisfeita precisamente pelas estruturas finitas. De fato, há conjuntos A_n de todas as cardinalidades $0 < n < \omega$, com $A_n \models \exists^{\geqslant k} x\, (x = x)$ para $k \leqslant n$. Suponha ainda que todos $A_n \models \sigma$. Então o conjunto $\{\sigma\} \cup \{\exists^{\geqslant k} x\, (x = x) \mid k \in \mathbb{N}\}$ é finitamente satisfazível, tendo um modelo infinito realizando σ.

Exemplo 1.1.3 (Remoção de constantes e operadores). Em algumas situações, veremos que será melhor supor que L contém apenas predicados, sem constantes ou operadores. Descreveremos breve e informalmente um meio de transformar L sem "perdas". Substitua cada constante c por um predicado unário, interpretado em uma L-estrutura $\mathfrak{A}$ como $\{c^{\mathfrak{A}}\}$, e cada operador n-ário f por um predicado $(n+1)$-ário, interpretado como o gráfico de $f^{\mathfrak{A}}$. Obtemos uma nova linguagem L^* e uma L^*-estrutura $\mathfrak{A}^*$. Ao custo de variáveis extras, cada fórmula de L pode ser reescrita como fórmula de L^*, sendo a definição de satisfação transferida adequadamente de $\mathfrak{A}$ para $\mathfrak{A}^*$. Imersões e isomorfismos não perdem suas propriedades definidoras. Por exemplo, se S é o predicado ternário para soma e Z o predicado unário para 0, então $\exists w\, (Z(w) \wedge \forall v\, S(v, w, v))$ corresponde a $\forall v\, (v + 0 = v)$.

Apresentamos agora alguns resultados muito úteis. O primeiro será reescrito em termos de subconjuntos definíveis e o segundo, por ser de uso tão freqüente na teoria, raramente é referido pela literatura.

Fato 1.1.4 (Tarski–Vaught). Suponha que $\mathfrak{A} \subseteq \mathfrak{B}$. Então $\mathfrak{A} \prec \mathfrak{B}$ se e somente se, para quaisquer fórmula $\phi(v, v_1, \ldots, v_n)$ e $a_1, \ldots, a_n \in A$ de modo que $\mathfrak{B} \models \exists v\, \phi(v, a_1, \ldots, a_n)$, existe $a \in A$ tal que $\mathfrak{B} \models \phi(a, a_1, \ldots, a_n)$.

Referências: A Proposição 3.1.2 de [Chang, Keisler] ou o Teorema 2.5.1 de [Hodges].

Exemplo 1.1.5. Na linguagem das ordens, $\mathbb{Q} \prec \mathbb{R}$.

Suponha $\phi(v, v_1, \ldots, v_n)$ e $a_1, \ldots, a_n \in \mathbb{Q}$ tais que $\mathbb{R} \models \exists v\, \phi(v, a_1, \ldots, a_n)$ como no enunciado. Existe então $x \in \mathbb{R}$ tal que $\mathbb{R} \models \phi(x, a_1, \ldots, a_n)$. Caso $x \in \mathbb{Q}$, não há nada a fazer. Se $x \notin \mathbb{Q}$, como $\mathbb{Q}$ é denso em $\mathbb{R}$ e $n < \omega$, existe $r \in \mathbb{Q}$ que satisfaz com $a_1, \ldots, a_n$ as mesmas relações de ordem que x, todas estritas. Por exemplo, se $a_5 < x < a_2$ então $a_5 < r < a_2$. Defina um automorfismo de ordem de $\mathbb{R}$ que fixe cada $a_1, \ldots, a_n$ e leve x a r, com uma bijeção crescente no intervalo em que x e r estão. Por esse automorfismo, $\mathbb{R} \models \phi(r, a_1, \ldots, a_n)$, bastando aplicar o fato.

Fato 1.1.6 (União de cadeia). Sejam $(I, \leqslant)$ um conjunto-índice linearmente ordenado e $\mathfrak{A}_i$, $i \in I$, L-estruturas tais que se $i \leqslant j$ então $\mathfrak{A}_i \subseteq \mathfrak{A}_j$, ou seja, as estruturas formam uma *cadeia*. É única a L-estrutura $\mathfrak{A}$ que satisfaz $A = \bigcup_{i \in I} A_i$ e $\mathfrak{A}_i \subseteq \mathfrak{A}$ para todo $i \in I$; indica-se $\mathfrak{A} = \bigcup_{i \in I} \mathfrak{A}_i$. Se ainda $\mathfrak{A}_i \prec \mathfrak{A}_j$ quando $i \leqslant j$, então $\mathfrak{A}_i \prec \mathfrak{A}$ para todo $i \in I$, chamando-se a cadeia *elementar*.

Referências: O parágrafo antecedendo o Lema 3.1.8 e o Teorema 3.1.9 de [Chang, Keisler] ou a pág. 49 e o Teorema 2.5.2 de [Hodges]. Esse resultado também é devido a Tarski e Vaught na formulação mais geral de *limites diretos*.

Fato 1.1.7 (Amalgamação). Se $\mathfrak{A} \equiv \mathfrak{B}$, então existem uma estrutura $\mathfrak{C}$ e imersões elementares de $\mathfrak{A}$ e $\mathfrak{B}$ em $\mathfrak{C}$. *Atenção: este é apenas um de muitos teoremas chamados "de Amalgamação".*

Referências: A Proposição 3.1.4 de [Chang, Keisler] ou o Teorema 6.4.1 de [Hodges].

Exemplo 1.1.8 (Estruturas finitas). Se $\mathfrak{A}, \mathfrak{B}$ são duas L-estruturas finitas com $\mathfrak{A} \equiv \mathfrak{B}$, então $\mathfrak{A} \cong \mathfrak{B}$. Para tanto, sejam $f : \mathfrak{A} \to \mathfrak{C}$ e $g : \mathfrak{B} \to \mathfrak{C}$ imersões elementares como dadas pelo fato. Então $|A| = |C|$, porque $\mathfrak{C} \models \exists^{=|A|} v\, (v = v)$; por $|A| < \omega$ e f ser injetora, concluímos que f é bijetora. Do mesmo modo, g é bijetora e, por definição, $g^{-1} \circ f$ é um isomorfismo entre $\mathfrak{A}$ e $\mathfrak{B}$.

A Teoria dos Modelos Finitos é extremamente importante, relacionando-se a questões de Decidibilidade e Complexidade Computacional, mas suas ferramentas estão atualmente dissociadas das que usaremos, em geral por causa da categoricidade da relação $\equiv$.

Dizemos que uma sentença σ é *conseqüência* de um conjunto de sentenças Σ e indicamos $\Sigma \models \sigma$ se todo modelo de Σ satisfizer σ. Se ϕ é uma fórmula qualquer, a terminologia refere-se ao fecho de ϕ. Essa relação tem uma contra-parte semi-recursiva no conceito de *prova formal*, sendo a correspondência completa conseqüência do importante Teorema da Completude de Gödel–Malcev–Henkin. Não trabalharemos com a noção de prova formal, de modo que a Completude perde seu significado. Contudo, esta conseqüência revelou-se muito mais útil:

Teorema 1.1.9 (Compacidade). Um conjunto de sentenças tem modelo se e somente se é *finitamente satisfazível!sentenças, conjunto de*, isto é, se cada um de seus subconjuntos finitos tem modelo.

Referências: O Teorema 1.3.22 de [Chang, Keisler] ou o Teorema 6.1.1 de [Hodges]. O Corolário 4.1.11 de [Chang, Keisler] e o Teorema 9.5.9 de [Hodges] apresentam demonstrações por meio de ultraprodutos, sem recorrer à Completude.

Tal discussão indica a importância das *teorias*, conjuntos consistentes de sentenças — por *consistente*, entendemos o mesmo que *satisfazível*, ou seja, ter um modelo.

Na linguagem das ordens, por exemplo, o leitor pode escrever as sentenças das teorias das ordens parciais; lineares ou totais; densas; sem primeiro ou último elemento, ou seja, sem extremidades. Com a ordem usual, $\mathbb{Q}$ é um modelo de todas essas sentenças.

Vemos que uma teoria T é maximal, com respeito a inclusão e dentre as teorias da mesma linguagem, se e somente se, para cada sentença σ dessa linguagem, $\sigma \in T$ ou $\neg\sigma \in T$, exclusivamente pela consistência. Desse modo, uma teoria maximal T da linguagem L tem cardinalidade $|T| = |\mathrm{L}|$.

Por exemplo, dada uma L-estrutura $\mathfrak{A}$, o conjunto $Th(\mathfrak{A})$ de sentenças de L válidas em $\mathfrak{A}$ é uma teoria de L. Vemos que os modelos de $Th(\mathfrak{A})$ são precisamente as estruturas elementarmente equivalentes a $\mathfrak{A}$. Além disso, pela definição de satisfação, $Th(\mathfrak{A})$ contém uma sentença de L ou sua negação, exclusivamente: então $Th(\mathfrak{A})$ é maximal. Assim, toda teoria estende-se a outra maximal, fato conhecido como Teorema de Lindenbaum, bastando tomar $Th(\mathfrak{A})$ para um modelo $\mathfrak{A}$ da teoria.

Uma teoria T é *completa* se todos os seus modelos são elementarmente equivalentes. Assim, T é completa se e somente se, para cada sentença σ da linguagem de T, ou $T \models \sigma$ ou $T \models \neg\sigma$. Teorias maximais são, portanto, completas. Lembramos que alguns textos reservam o termo "teoria" apenas para teorias completas ou maximais. Por exemplo, verifica-se que a teoria das ordens lineares densas sem extremidades é completa.

Duas teorias completas (da mesma linguagem) com um modelo comum têm, de fato, todos os seus modelos em comum. Em particular, se T é completa e $\mathfrak{A} \models T$, então T e $Th(\mathfrak{A})$ têm os mesmos modelos, fato freqüentemente implícito na transposição de definições entre estruturas e teorias completas.

Também por esse motivo, é costumeiro incluir em uma teoria completa T todas as suas conseqüências. Assim, $|T| = |\mathrm{L}|$ na literatura em geral.

Note ainda que se uma teoria completa tem modelos infinitos, então todos os seus modelos são infinitos.

A teoria $Th(\mathfrak{A}, (a)_{a\in A})$ de $\mathrm{L}(A)$ é chamada o *diagrama elementar* de $\mathfrak{A}$. Dado um modelo seu $(\mathfrak{B}, (b_a)_{a\in A})$, a função $h : \mathfrak{A} \to \mathfrak{B}$, $h(a) = b_a$, é uma imersão elementar e, reciprocamente, as estruturas em que $\mathfrak{A}$ pode ser elementarmente imersa são modelos de $Th(\mathfrak{A}, (a)_{a\in A})$ interpretando-se as novas constantes como suas imagens pela imersão.

Note que, nesta situação, não podemos omitir $(x)_{x\in X}$ em $Th(\mathfrak{A}, (x)_{x\in X})$.

Uma teoria T é *modelo-completa* se toda imersão entre modelos de T é elementar. Isso equivale a, para cada modelo $\mathfrak{A} \models T$, a teoria $T \cup D(\mathfrak{A})$ ser completa na linguagem $\mathrm{L}(A)$, sendo L de T e $D(\mathfrak{A})$ o *diagrama* de $\mathfrak{A}$, isto é, a teoria das sentenças atômicas ou negações de atômicas de $\mathrm{L}(A)$ válidas em $(\mathfrak{A}, (a)_{a\in A})$. Para tanto, mostra-se que $\mathfrak{A}$ é imersível em $\mathfrak{B}$ se e somente se $\mathfrak{B} \models D(\mathfrak{A})$ com alguma interpretação para as novas constantes.

Um modelo $\mathfrak{A} \models T$ é um *modelo algebricamente primo* de T se todo modelo de T tem subestrutura isomorfa a $\mathfrak{A}$; é dito simplesmente *modelo primo* de T se é elementarmente imersível em todo modelo de T.

Duas fórmulas ϕ, ψ são *equivalentes* em uma estrutura se esta for modelo do fecho de $\phi \leftrightarrow \psi$. Diz-se que ϕ e ψ são *equivalentes em uma teoria* T se o forem em todo modelo de T. Na notação desenvolvida, se v é uma seqüência de variáveis incluindo as livres em ϕ ou ψ, temos $T \models \forall v\,(\phi(v) \leftrightarrow \psi(v))$, ou mais simplesmente $T \models \phi \leftrightarrow \psi$.

Uma teoria T admite *eliminação de quantificadores* se para cada fórmula ϕ existe outra equivalente a ϕ em T, sem quantificadores e sem outras variáveis livres além das de ϕ. Nesse caso, a eliminação estende-se a fórmulas de $\mathrm{L}(A)$ para equivalência em $\mathfrak{A} \models T$, bastando substituir as novas constantes por novas variáveis para eliminar os quantificadores. Novamente, sabe-se que é um exemplo a teoria das ordens lineares densas sem extremidades.

Para evitar considerações sobre sentenças sem quantificadores — que somente existem em linguagens com constantes —, alguns autores assumem que ϕ tenha ao menos uma variável livre. Não precisaremos de tal exatidão.

A Seção 1.5 de [Chang, Keisler] e a Seção 2.7 de [Hodges] apresentam o conceito em forma ampla, que aqui não será necessária, mas bastante usada na Teoria dos Modelos e em Decidibilidade.

Na próxima seção, esses conceitos serão exemplificados pela teoria dos corpos algebricamente fechados. O leitor encontrará, em nossas referências, seções homônimas às definições e que demonstram tais propriedades para diversas teorias.

Como curiosidade, citamos o procedimento canônico e simples de expandir-se uma linguagem a outra para que haja eliminação de quantificadores. Para cada fórmula ϕ de n variáveis livres, adicionamos um predicado n-ário P_ϕ, ao qual imporemos que essa fórmula equivalha (adicionando o fecho de $\phi \leftrightarrow P_\phi$ aos axiomas da teoria). Cada fórmula da nova linguagem equivale a uma fórmula da antiga, obtida substituindo-se os novos predicados P_ϕ por suas fórmulas originais ϕ; por sua vez, esta fórmula equivale a um novo predicado.

Lembrando que imersões preservam a validade de fórmulas sem quantificadores, obtemos

Fato 1.1.10. Toda teoria que tem eliminação de quantificadores é modelo-completa.

Todos os quatro resultados deste teorema são coletivamente chamados Teorema de Löwenheim–Skolem, freqüentemente com os rótulos "para baixo" e "para cima". São os primeiros teoremas da Teoria dos Modelos, na forma atual devidos a Tarski.

Teorema 1.1.11. (i) Sejam $\mathfrak{A}$ uma L-estrutura e $X \subseteq A$. Para todo cardinal β que satisfaça $|X|, |\mathrm{L}| \leqslant \beta \leqslant |A|$, existe uma estrutura $\mathfrak{B}$ de cardinal β tal que $\mathfrak{B} \prec \mathfrak{A}$ e $X \subseteq B$.

(ii) Toda teoria de L tem um modelo de cardinal no máximo $|\mathrm{L}|$.

(iii) Seja $\mathfrak{A}$ uma L-estrutura infinita. Para todo cardinal β que satisfaça $\beta \geqslant |A|, |\mathrm{L}|$, existe uma estrutura $\mathfrak{B}$ de cardinal β tal que $\mathfrak{A} \prec \mathfrak{B}$.

(iv) Se uma teoria de L tem modelos infinitos, então tem modelos de qualquer cardinalidade $\geqslant |\mathrm{L}|$.

Referências: (i) O Teorema 3.1.6 de [Chang, Keisler] ou o Corolário 3.1.5 de [Hodges]. O início da Seção 3.1 de [Hodges] sumariza a demonstração usual.

(ii) é facilmente derivado de (i), mas também é uma forma da Completude.

(iii) O Corolário 6.1.4 de [Hodges]. Este resultado também pode ser deduzido de (iv), por meio de $Th(\mathfrak{A}, (a)_{a\in A})$.

(iv) O Corolário 2.1.6 de [Chang, Keisler], que envolve apenas (ii) e a Compacidade. Novamente, pode ser deduzido de (iii), usado primeiro em seqüência a (i) para obter um modelo de cardinalidade $|\mathrm{L}|$.

O item (iii) permite obter, sem maiores detalhes, extensões elementares próprias de estruturas infinitas. Na demonstração do Teorema 1.4.11, precisaremos do Exercício 6.1.11 de [Hodges], que colocamos como um

Adendo. Em (iii), se ainda $\beta = |A| \geqslant |\mathrm{L}|$, podemos assumir $|B - A| = |A|$, mas não $0 < |B - A| < |A|$.

Demonstração: Tome C um conjunto de novas constantes, com $A \cap C \neq \emptyset$ e $|C| = |A|$. Então $|\mathrm{L}(A \cup C)| = |\mathrm{L}| + |A| + |C| = |A|$. Tome $T = Th(\mathfrak{A}, (a)_{a\in A}) \cup \{c \neq a \mid c \in C,\ a \in A\}$. Esse conjunto de sentenças é finitamente satisfazível, bastanto interpretar em $\mathfrak{A}$ as novas constantes de C por elementos que não ocorram como constantes de A no número finito de sentenças, sendo A infinito. Então T tem um modelo $(\mathfrak{B}, (b_a)_{a\in A}, (b_c)_{c\in C})$, que podemos supor de cardinal $|A|$. Temos $\mathfrak{A}$ elementarmente imersa em $\mathfrak{B}$. Mas $|B - A| \geqslant |C|$ porque todas as constantes de C são distintas das de A, de modo que $|B - A| = |A|$.

Como contra-exemplo para o caso $0 < |B - A| < |A|$, retomamos o Exemplo 1.1.1, em que vimos que os novos elementos de uma extensão elementar de $\mathbb{N}$, com sua ordem usual, são em número infinito. É claro que podemos ter $|B - A| = 0$, tomando $\mathfrak{B} = \mathfrak{A}$. QED

Suponha que Φ é um conjunto de fórmulas de L com variáveis livres dentre $v_1, \ldots, v_n$. Usa-se a notação $\Phi(v_1, \ldots, v_n)$ com o mesmo significado que para uma única fórmula.

Por exemplo, sendo $\mathfrak{A}$ uma L-estrutura e $a_1, \ldots, a_n \in A$, indica-se $\mathfrak{A} \models \Phi(a_1, \ldots, a_n)$ se e somente se $\mathfrak{A} \models \phi(a_1, \ldots, a_n)$ para toda $\phi \in \Phi$. Diz-se que, nesse caso, $(a_1, \ldots, a_n)$ *realiza* Φ em $\mathfrak{A}$.

Dizemos que $\mathfrak{A}$ *realiza* Φ e Φ é *satisfazível* em $\mathfrak{A}$ se existe $(a_1, \ldots, a_n) \in A^n$ que realiza Φ em $\mathfrak{A}$. Caso isso não ocorra, dizemos que $\mathfrak{A}$ *omite* Φ.

Finalmente, Φ é *consistente* se satisfazível em alguma estrutura e *consistente com uma teoria* T se satisfazível em algum modelo de T. Desse modo, Φ ***não*** é tratado como um conjunto de axiomas dos quais bastaria tomar os fechos; o mesmo se aplica a uma única fórmula.

Assim, Φ pode ser *finitamente satisfazível!fórmulas, conjunto de*, quando cada seu subconjunto finito é satisfazível em alguma estrutura. Substituindo as variáveis livres por novas constantes, podemos aplicar o Teorema da Compacidade para concluir que Φ é satisfazível por inteiro. Eis o que ocorre quando a estrutura é sempre a mesma:

Corolário 1.1.12 (Compacidade). Considere $\Phi(v_1, \ldots, v_n)$ um conjunto de fórmulas e $\mathfrak{A}$ uma estrutura da linguagem adequada. Se $\mathfrak{A} \models \exists v_1 \ldots \exists v_n \bigwedge \Phi_0$ para todo Φ_0 subconjunto finito não-vazio de Φ, então existe uma extensão elementar de $\mathfrak{A}$ que realiza Φ.

Demonstração: Adicione a $L(A)$ novas constantes $c_1, \ldots, c_n$, obtendo a linguagem $L(A)'$. Seja $\Phi(c_1, \ldots, c_n)$ o conjunto de sentenças obtido de Φ substituindo-se cada v_i pela constante c_i.

Observe que, se $(a_1, \ldots, a_n)$ realiza Φ_0, então $Th(\mathfrak{A}, (a)_{a \in A}) \cup \Phi_0(c_1, \ldots, c_n)$ é satisfeito pela $L(A)'$-estrutura $(\mathfrak{A}, (a)_{a \in A}, a_1, \ldots, a_n)$, em que cada a_i interpreta c_i. Assim, $T = Th(\mathfrak{A}, (a)_{a \in A}) \cup \Phi(c_1, \ldots, c_n)$ é finitamente satisfazível.

Pelo Teorema da Compacidade, T tem um modelo $(\mathfrak{B}, (b_a)_{a \in A}, b_1, \ldots, b_n)$. Então $(b_1, \ldots, b_n)$ realiza Φ em $\mathfrak{B}$ e $\mathfrak{A}$ é elementamente imersível em $\mathfrak{B}$. QED

1.2. O exemplo principal: Álgebra

As estruturas com que mais trabalharemos são os grupos e os corpos, entre outras algébricas. Aproveitaremos esta seção para visualizá-los sob a teoria desenvolvida e agrupar os conceitos específicos de que faremos uso. De fato, concentrar-nos-emos nos corpos, apenas fixando a linguagem dos grupos e fazendo um breve comentário sobre módulos. Dentre todos os corpos, também privilegiaremos os algebricamente fechados como exemplo em todo o texto, destacando o Capítulo 8 para estudar outras classes de corpos que se farão úteis.

Sugerimos como referências, em Álgebra, os dois volumes [Jacobson I] e [Jacobson II] ou o único [Lang], embora não requeiramos que o leitor domine todo o seu conteúdo. Necessitaremos apenas, de início, conceitos básicos sobre os quais o leitor pode consultar seu texto favorito.

A linguagem apropriada para os corpos tem duas constantes, 0 e 1, dois operadores binários (infixos), $+$ e $.$, e dois operadores unários (prefixos), $-$ e $^{-1}$. Omitiremos parênteses correspondentes à precedência usual e à associação da esquerda para a direita e também o símbolo da segunda operação, indicando-a pelo modo usual de justaposição. Além disso, usaremos a subtração binária $-$ e a barra de divisão / quando conveniente.

As sentenças da teoria dos corpos são os fechos destas fórmulas: $x+y = y+x$, $xy = yx$, $x + (y + z) = (x + y) + z$, $x(yz) = (xy)z$, $0 + x = x$, $1x = x$, $x(y+z) = xy+xz$, $x+(-x) = 0$, $x \neq 0 \rightarrow xx^{-1} = 1$, $0 \neq 1$. Note que 0^{-1} é um termo dessa linguagem e que, então, tem valor em toda estrutura apropriada.

Observamos que, devido ao fato da linguagem ter as constantes e operadores usuais (em vez de relações de soma e produto), a noção de subestrutura, aplicada a corpos, corresponde precisamente à noção de subcorpo usual. O leitor cuidadoso reparará que o termo 0^{-1} não necessariamente pertence a um subcorpo. Para tanto, convencionamos adicionar $0^{-1} = 0$ aos axiomas acima.

Quando trabalharmos com extensões, sem maiores comentários, assumiremos conformemente que se tratam também de corpos.

Desse modo, podemos simplificar a notação da Teoria dos Modelos para corpos, com os domínios denotando diretamente suas estruturas correspondentes, ou seja, escreveremos "um corpo L" em vez de "um corpo $\mathfrak{L}$". (A notação itálica é atualmente o padrão para quaisquer estruturas.) O mesmo se aplicará a grupos, anéis e estruturas análogas: deixamos a cargo do leitor as linguagens e axiomatizações adequadas.

Os números naturais podem ser introduzidos na linguagem dos corpos pelo modo natural e comum. Se $n = 0$ ou 1, $\overline{n}$ abrevia a constante 0 ou 1 respectivamente. Se $n > 1$, $\overline{n}$ abrevia $(\overline{n-1} + 1)$.

Para cada p natural primo, a sentença $\overline{p} = 0$ é satisfeita por corpos somente de característica p. Os corpos de característica 0 são aqueles que satisfazem $\{\overline{p} \neq 0 \mid p \text{ natural primo}\}$.

Podemos também introduzir a abreviatura t^n, para um termo t. Se $n = 0$, t^n abrevia a constante 1; se $n = 1$, t^n é o próprio termo (t); se $n > 1$, t^n abrevia $(t^{n-1}t)$.

Desse modo, somos naturalmente induzidos a identificar um polinômio $f \in R[x_1, \ldots, x_n]$, em que R é um anel qualquer, com o termo de n variáveis livres e parâmetros de R correspondente, que escreveremos $f(v_1, \ldots, v_n)$.

Podemos estender as abreviaturas $\overline{n}$ e t^n a $n \in \mathbb{Z}$: para $n < 0$, $\overline{n}$ abrevia $-\overline{-n}$ e t^n abrevia $(t^{-1})^{-n}$. Mais ainda, podemos introduzir todos os racionais: se $p, q \in \mathbb{Z}$, $q \neq 0$ e $r = \frac{p}{q}$, então $\overline{r}$ abrevia $(\overline{p}(\overline{q})^{-1})$. Em corpos de característica 0, esses termos têm as interpretações usuais.

Omitiremos a barra $^{-}$.

Com essas convenções, a teoria dos corpos algebricamente fechados é obtida adicionando-se aos axiomas de corpo as sentenças $\forall x_0 \ldots \forall x_{n-1} \exists y\, (x_0 y^0 + \ldots + x_{n-1} y^{n-1} + y^n = 0)$ para $n \geqslant 2$. Chamaremos a essa teoria ACF (em inglês, *algebraically closed fields*). Sejam ainda ACF_0 a teoria dos corpos algebricamente fechados de característica 0 e ACF_p a daqueles de característica p prima.

Atentemos agora para um fato peculiar envolvendo o operador $^{-1}$. Nessa linguagem, os termos (por exemplo $(\frac{1}{x} - \frac{x+y}{y})/(z(1+\frac{1}{x}))$) correspondem a funções racionais (quocientes de polinômios; no caso $(y - x(x+y))/(xyz + yz)$). Em algumas ocasiões, tais termos dificultam o trabalho. Retirando-se o operador $^{-1}$, obtemos a linguagem dos anéis com unidade, para os quais subestruturas correspondem a subanéis com unidade e isomorfismos a isomorfismos de anéis com unidade. As abreviaturas acima não sofrem qualquer alteração, mas os termos passam a ser simples polinômios (por exemplo $x + 1 - (y + 1)z$). Porém, nessa linguagem, a relação de inverso é definível: dois elementos a, b em um corpo satisfazem $\phi(x, y) : (x = y = 0) \vee (xy = 1)$ se e somente se são ambos nulos ou $b = a^{-1}$. Assim, $\forall x \exists y\, \phi(x, y)$ substitui na teoria dos corpos o axioma de inversão.

Portanto, para raciocinar sobre corpos, trabalharemos apenas com a linguagem de anéis com unidade. Note que os isomorfismos entre corpos são exatamente os isomorfismos nessa linguagem, ou ainda os isomorfismos na linguagem com inversão.

Assim, com termos correspondendo a polinômios, sabemos que fórmulas atômicas são sempre da forma $t = t'$ e podemos, com $t - t' = 0$, limitarmo-nos ao caso $t = 0$, ou seja, a discutir raízes de polinômios. Veja, por exemplo, o Exemplo 1.3.6. (Pode-se também, com $t = 0$, racionalizar o termo e considerar o numerador nulo.)

Teorema 1.2.1 (Tarski). *ACF* tem eliminação de quantificadores na linguagem dos anéis com unidade.

Referências: O Teorema 3.2.2 de [Marker] ou o Teorema 6.4 de [Poizat 1]. O leitor interessado não deve sentir-se desestimulado pelo comprimento da demonstração: embora a modelo-completude seja uma conseqüência da eliminação de quantificadores, é primeiro demonstrada para depois ser usada no raciocínio.

A maioria das propriedades de *ACF* que estudaremos são conseqüências desse resultado, até mesmo enunciados centrais da Álgebra, como o Teorema de Tarski–Chevalley (Teorema 6.1.9) e o *Nullstellensatz* de Hilbert (Teorema 6.1.10). Toda teoria de corpos infinitos com eliminação de quantificadores nessa linguagem contém *ACF*, pelo Teorema de Macintyre (veja o Corolário 5.7.3).

Façamos uma breve observação que nos apoiará futuramente e que esclarece o poder das linguagens escolhidas.

Sejam L um corpo, X um subconjunto qualquer de L e K o subcorpo de L *gerado por* X, isto é, a intersecção de todos os subcorpos de L que contêm X. Considere os elementos de L que são os valores dos termos da linguagem dos corpos quando suas variáveis têm valores em X: chamaremos esses elementos como *obtidos de* X *por termos*. É fácil ver que K é o conjunto dos elementos obtidos de X por termos. Primeiramente, como K contém X e é um subcorpo de L, contém esses elementos. Por outro lado, o conjunto desses elementos contém X e é um subcorpo de L, pois é fechado sob $+$, $.$, $-$, $^{-1}$ e contém $0, 1$, de modo que contém K.

No caso da linguagem dos anéis com unidade, o subanel com unidade gerado é analogamente o conjunto dos elementos obtidos por termos, de modo que K é seu corpo de frações.

Note ainda que (i) os automorfismos de L sobre K são também sobre X, porque $X \subseteq K$, e (ii) os automorfismos de L sobre X são também sobre K, porque o são sobre o subanel gerado por X, cujos elementos são obtidos por termos polinomiais, e portanto sobre seu corpo quociente. Em outras palavras, o grupo de automorfismos sobre X é o mesmo sobre K.

Notamos também que os corpos primos são modelos algebricamente primos das teorias dos corpos com suas características, ou seja, $\mathbb{Q}$ está imerso em todo corpo de característica 0 e o corpo de p elementos em todos os de característica p prima. As imagens dos corpos primos são os subcorpos gerados por $\emptyset$. No caso das teorias ACF_0, ACF_p, os fechos algébricos correspondentes são os modelos algebricamente primos, simplesmente primos pela modelo-completude de ACF. Assim, as teorias ACF_0, ACF_p são completas.

Concluímos com alguns fatos úteis.

Suponha $K \subseteq L$ dois corpos e $\emptyset \neq S \subseteq L$.

Se S é finito, escreva $S = \{s_1, \ldots, s_k\}$ sem repetições. Diz-se que S é *algebricamente independente* sobre K se o único polinômio $p \in K[x_1, \ldots, x_k]$ com $p(s_1, \ldots, s_k) = 0$ é o nulo $p = 0$. Por exemplo, todo conjunto unitário de elemento transcendente sobre K é algebricamente independente.

Se S é infinito, diz-se que S é *algebricamente independente* sobre K se todo seu subconjunto finito o for.

S é uma *base de transcêndencia* de L sobre K se S é algebricamente independente e L é extensão algébrica de $K(S)$. Diz-se então que $K(S)$ é *extensão transcendental pura* de K.

Sabe-se que bases de transcendência existem para qualquer extensão $K \subseteq L$, e quaisquer duas têm a mesma cardinalidade, chamada o *grau de transcendência* de L sobre K. Referimos o leitor ao Teorema VIII.1.1 de [Lang] ou ao Teorema 8.35 de [Jacobson II].

Se B é uma tal base, então nenhum elemento $b \in B$ é algébrico sobre $K(B - \{b\})$, como mostra o Teorema 8.33 de [Jacobson II] ou o Lema anterior ao Teorema 1.8 do Capítulo 5 do livro de J. K. Goldhaber, G. Ehrlich, *Algebra*, 2ª impressão, The Macmillan Company, 1971.

Suponha agora $K \subseteq E \subseteq L$ corpos, com L algebricamente fechado e o grau de transcendência de E sobre K finito. Então toda imersão de E em L que fixa os elementos de K estende-se a um automorfismo de L: remetemos o leitor ao Corolário 2 do Teorema 2.5 do mesmo capítulo de Goldhaber e Ehrlich. Podemos identificar dois casos particulares:

Se $a \in L$ é algébrico sobre K, então $K(a)$ é uma extensão algébrica de K e seu grau de transcendência é 0. Suponha $b \in L$ também raiz do polinômio minimal de a sobre K. Sabemos que existe um isomorfismo de $K(a)$ a $K(b)$ fixando os elementos de K e levando a a b. Obtemos um automorfismo de L sobre K pelo qual a tem imagem b.

Se $a \in L$ é transcendente sobre K, então $K(a)$ é uma extensão puramente transcendental de K com base $\{a\}$ e grau 1. Suponha $b \in L$ também transcendente sobre K. Pelos isomorfismos naturais entre $K(a)$ ou $K(b)$ e o corpo quociente do anel $K[x]$, existe um isomorfismo de $K(a)$ a $K(b)$ fixando os elementos de K e levando a a b. Obtemos um automorfismo de L sobre K pelo qual a tem imagem b.

Vemos que esses são também os únicos casos possíveis para $a, b \in L$ serem conjugados por um automorfismo sobre K.

Seja agora F um corpo qualquer de característica p prima. A *função de Frobenius* $\varphi : F \to F$, $\varphi(x) = x^p$, é uma imersão de corpos, aditiva e injetora porque $(x \pm y)^p = x^p \pm y^p$ — os outros coeficientes binomiais são divisíveis por p. Observamos que φ é $\emptyset$-definível e sua inversa $\varphi^{-1}\varphi[F] \to F$ também. Definem-se $F^{p^n} = \varphi^n[F]$, em que φ^n é a composição n vezes de φ (φ^0 é a identidade), e $F^{p^\infty} = \bigcap_{n \in \mathbb{N}} F^{p^n}$.

Corpos perfeitos admitem muitas caracterizações; portanto, optamos por apresentar aquelas que se fizerem necessárias enquanto pedimos ao leitor que reconheça a sua favorita. Primeiramente, um corpo é perfeito quando nenhum polinômio irredutível com coeficientes nesse corpo tem raízes múltiplas em qualquer extensão. É precisamente o caso dos corpos de característica 0 e dos corpos de característica positiva em que a função de Frobenius é sobrejetora.

A linguagem dos corpos ordenados

Adicionando-se à linguagem dos anéis com unidade (ou dos corpos) um predicado binário $\leqslant$, obtém-se a linguagem dos corpos ordenados, cujos axiomas são as sentenças (i) da teoria dos corpos; (ii) da teoria das ordens lineares ou totais; (iii) $\forall x \forall y \forall z\, (x < y \to x + z < y + z)$, $\forall x \forall y \forall z\, ((x < y \wedge z > 0) \to xz < yz)$.

A linguagem dos grupos

Esta linguagem tem dois operadores, de adição/produto e oposto/inverso, e a constante de elemento neutro. Desse modo, as subestruturas de um grupo são precisamente seus subgrupos e os isomorfismos entre grupos são isomorfismos de grupos. Fazem-se, para esta linguagem, as mesmas convenções e abreviaturas que para a linguagem dos corpos.

Espaços vetoriais e módulos

Quando generalizamos o conceito de "K-espaço vetorial" substituindo o corpo K por um anel R (com unidade), obtemos um "R-módulo". O leitor pode encontrar os axiomas explícitos na Seção III.1 de [Lang] ou na Seção 3.2 de [Jacobson II], enquanto aqui faremos apenas uma consideração. Se M é um candidato a R-módulo e $x \in M$, $r, s \in R$, uma das propriedades de espaços vetoriais escreve-se $r(sx) = (rs)x$. Porém, R não sendo necessariamente comutativo, podemos considerar também $r(sx) = (sr)x$. Neste caso, escreve-se o produto à direita, de modo que $(xs)r = x(sr)$. Distingüem-se, assim, os R-módulos à esquerda e à direita.

Surge a questão de qual linguagem é apropridada para os módulos e os espaços vetoriais. Uma abordagem, comum a outras situações em que ainda é muito útil, toma como domínio da estrutura R-módulo M a união disjunta de R e M, estipula que dois predicados unários identifiquem R e M e inclui axiomas de que são disjuntos e sua união é todo o domínio, além de escrever os axiomas das operações identificando as variáveis: "Para todos x, r, se x é um vetor e r é um escalar...". Embora operacional, essa solução complica os estudos de cardinalidades e imersões elementares, entre outros.

Atualmente, recorre-se ao expediente de fixar o anel R e providenciar, para cada $r \in R$, um operador correspondendo ao produto por r. Assim, as estruturas que representam R-módulos têm efetivamente o domínio de R-módulos. Quando se toma uma extensão elementar, ou um isomorfismo, ainda se trabalha com o mesmo anel R, que na primeira solução poderia ser modificado. Note, também, que o operador rs deve então ser axiomatizado como a composição de r e s.

A respeito de módulos em Teoria dos Modelos, um estudo muito frutífero, veja a Seção A.1 de [Hodges] ou a Seção 6.5 e o Exemplo 16 na Seção 13.3 de [Poizat 1].

1.3. Subconjuntos definíveis e tipos

Paralelamente a essa teoria *algébrica* de imersões e satisfação, desenvolve-se o estudo *geométrico* dos subconjuntos definíveis, que agora expomos. O conceito de conjunto definível corresponde ao de "lugar geométrico" na Geometria clássica. Também seremos naturalmente levados ao estudo dos ultrafiltros de definíveis, correspondentes a tipos.

Por toda a seção, sejam L uma linguagem arbitrária, $\mathfrak{A}$ uma L-estrutura e $X \subseteq A$.

Um subconjunto D de A^m é *definível* se existem $\phi(x_1, \ldots, x_m, y_1, \ldots, y_n)$ fórmula de L e $a \in A^n$ tais que

$$D = \phi(\mathfrak{A}, a) = \{\alpha \in A^m \mid \mathfrak{A} \models \phi(\alpha, a)\} .$$

Os elementos da n-upla a são ditos *parâmetros* Note que m é fixo, enquanto número de "coordenadas" de D, mas n é arbitrário, podendo mesmo ser $n = 0$.

Uma família de definíveis é *uniformemente definível* se o for por uma única fórmula, mas diferentes parâmetros.

Caso se queira indicar que todos os parâmetros pertencem a algum $X \subseteq A$, diz-se *X-definível* ou *definível sobre X*. Alguns textos escrevem "0-definível" em vez de "$\emptyset$-definível". É importante lembrar que, nessa notação, todo X-definível é definível, mas não reciprocamente, enquanto que em alguns textos "definível" corresponde a "$\emptyset$-definível".

Tais definições aplicam-se a um elemento $a \in A$ como subconjunto $\{a\}$ (ou seja, a fórmula é satisfeita apenas por a) e a uma função $f : R \longrightarrow S$, com $R \subseteq A^r$ e $S \subseteq A^s$, como gráfico $f \subseteq R \times S \subseteq A^r \times A^s = A^{r+s}$.

Observamos que fórmulas parametrizadas que definem um mesmo conjunto são equivalentes e identificamos totalmente os conjuntos definíveis com as fórmulas parametrizadas que os definem. Assim, podemos considerar um X-definível, uma fórmula de L e parâmetros em X, ou uma fórmula de L(X), digamos ϕ: seguindo nossa convenção, escreveremos $\phi(\mathfrak{A})$ em vez de $\phi(\mathfrak{A}, (x)_{x \in X})$. As definições que faremos a esses conjuntos são, na literatura em geral, feitas para as fórmulas que os definem.

Exemplo 1.3.1. Suponha L um corpo e K o subcorpo gerado por $X \subseteq L$. Toda fórmula com parâmetros em K reescreve-se equivalentemente como fórmula com parâmetros em X. Isso vale tanto na linguagem dos corpos, porque cada elemento de K é obtido de X por termos, como na que usamos, dos anéis com unidade. Nesse caso, adicionamos às fórmulas variáveis quantificadas existencialmente para escrever os quocientes dos elementos do subanel gerado por X. Por exemplo, suponha $x, y \in X$ com $y \neq 0$ e $\phi(v, w)$ uma fórmula com duas variáveis livres: então $x/y \in K$ e $\phi(v, x/y)$ equivale em L a $\psi(v, x, y) : \exists w\, (\phi(v, w) \wedge (x = wy))$, ou seja, $\phi(L, x/y) = \psi(L, x, y)$. Portanto, um subconjunto de L^m é definível sobre K se e somente se é definível sobre X, porque os elementos de K são X-definíveis; na notação abaixo, $\mathrm{Def}^m_{L,K} = \mathrm{Def}^m_{L,X}$.

Exploremos agora algumas das propriedades dos definíveis.

Dado $X \subseteq A$, seja $\mathrm{Def}^m_{\mathfrak{A},X}$ ou simplesmente Def^m_X a coleção dos subconjuntos X-definíveis de A^m. Observe que $\mathrm{Def}^0_X = \{\emptyset\}$; portanto, suporemos sempre $m \geqslant 1$. Trata-se de uma álgebra de Boole com as operações usuais de intersecção, união e complementação correspondendo respectivamente a conjunção, disjunção e negação de fórmulas; seu mínimo é $\emptyset$ definido por $\neg(v = v)$ e seu máximo é A^m definido por $v = v$. Note ainda que

$$\phi(\mathfrak{A}, a) \subseteq \psi(\mathfrak{A}, b) \Leftrightarrow \mathfrak{A} \models \forall v\, (\phi(v, a) \rightarrow \psi(v, b)) .$$

Se $X \subseteq Y \subseteq A$, lembramos que $\mathrm{Def}^m_X \subseteq \mathrm{Def}^m_Y$ como subálgebra.

Há também uma propriedade simples de álgebras de Boole: dado $D \in \mathrm{Def}^m_A$, os conjuntos $\{D \cap E \mid E \in \mathrm{Def}^m_A\}$ e $\{F \in \mathrm{Def}^m_A \mid F \subseteq D\}$ são idênticos.

Se $\xi : \mathfrak{A} \rightarrow \mathfrak{B}$ é um isomorfismo e $D = \phi(\mathfrak{A}, a)$ é um definível qualquer, então $\xi[D] = \phi(\mathfrak{B}, \xi(a))$: de fato,

$$\begin{aligned} b \in \phi(\mathfrak{B}, \xi(a)) &\Leftrightarrow \mathfrak{B} \models \phi(b, \xi(a)) \Leftrightarrow \\ &\Leftrightarrow \mathfrak{A} \models \phi(\xi^{-1}(b), a) \qquad \text{(pois } \xi \text{ é uma imersão elementar)} \\ &\Leftrightarrow \xi^{-1}(b) \in \phi(\mathfrak{A}, a) = D \Leftrightarrow b \in \xi[D] . \end{aligned}$$

Alguns resultados que vimos na primeira seção podem ter seus enunciados reescritos sobre definíveis. Por exemplo, o Fato de Tarski–Vaught implica

Corolário 1.3.2. Suponha que $\mathfrak{A} \subseteq \mathfrak{B}$. Então $\mathfrak{A} \prec \mathfrak{B}$ se e somente se, para todo A-definível não-vazio $D \subseteq B$ em $\mathfrak{B}$, também $A \cap D$ é não-vazio.

e do Corolário 1.1.12 conclui-se

Corolário 1.3.3. Suponha $\phi_i(\mathfrak{A}, a_i) \in \mathrm{Def}^m_A$, $i \in I$, uma família de definíveis em uma estrutura $\mathfrak{A}$ com a propriedade da intersecção finita, isto é, $\bigcap_{i \in I_0} \phi_i(\mathfrak{A}, a_i) \neq \emptyset$ para cada I_0 subconjunto finito de I. Então há uma extensão elementar $\mathfrak{B}$ de $\mathfrak{A}$ em que $\bigcap_{i \in I} \phi_i(\mathfrak{B}, a_i) \neq \emptyset$.

Note também que, se $\mathfrak{A} \prec \mathfrak{B}$ e ϕ é uma fórmula de $\mathrm{L}(A)$, então $\phi(\mathfrak{A}) \subseteq \phi(\mathfrak{B})$. Através das fórmulas $\exists^{=k}$, vemos que se $\phi(\mathfrak{A})$ ou $\phi(\mathfrak{B})$ é finito então $|\phi(\mathfrak{A})| = |\phi(\mathfrak{B})|$ e, assim, $\phi(\mathfrak{A}) = \phi(\mathfrak{B})$. As operações de união, intersecção e complementação são preservadas sob imersões elementares e frisamos que a mesma fórmula $x = x$ define o domínio em qualquer estrutura.

Este fato resume diversas propriedades dos definíveis e também permite uma construção alternativa da teoria, sem uso de fórmulas, bastante usada em artigos. Atentamos para as propriedades (iv), (vi) e (vii). Na forma restrita, entre parênteses, (iv) corresponde à adição de variáveis mudas. As projeções em (vi) podem ser de várias formas: projeções usuais, permutações ou repetições de coordenadas (variáveis) ou todas essas possibilidades simultaneamente. (vii) permite *especializar* ou tomar *fibras*. Note que n pode ser menor, igual ou até maior que m; em alguns itens, temos $m, n > 0$.

Fato 1.3.4. Considere, para cada $m \in \mathbb{N}^*$, um conjunto D_m de subconjuntos de A^m. Os conjuntos Def_A^m são os menores possíveis com as propriedades listadas a seguir, de modo que cada $D_m = \mathrm{Def}_A^m$.

(i) Para cada predicado n-ário de L, sua interpretação pertence a D_n; para cada operador n-ário de L, o gráfico de sua interpretação pertence a D_{n+1}; para cada constante de L, o conjunto unitário de sua interpretação pertence a D_1.

(ii) Para quaisquer $1 \leqslant i, j \leqslant m$, a *diagonal* $\{(a_1, \dots, a_m) \in A^m \mid a_i = a_j\}$ pertence a D_m. (Em particular, $A^m \in D_m$.)

(iii) Se $D \in D_m$ e $E \in D_n$ então $D \times E \in D_{m+n}$. (Basta $D \times A \in D_{m+1}$.)

(iv) Cada D_m é fechado sob complementação, intersecção e união, ou seja, é uma álgebra de Boole com as operações usuais.

(v) Se $D \in D_m$ e $\pi : A^m \to A^n$, $\pi(a_1, \dots, a_m) = (a_{i_1}, \dots, a_{i_n})$, é uma *projeção* qualquer, então $\pi[D] \in D_n$.

(vi) Se $D \in D_{m+n}$ e $a \in A^n$, então $\{\alpha \in A^m \mid (\alpha, a) \in D\} \in D_m$.

As propriedades (iii), (iv) e (v) valem também para $(\mathrm{Def}_X^m)_{m \in \mathbb{N}^*}$ — essas operações a conjuntos X-definíveis resultam em X-definíveis — e a propriedade (vi) vale também para Def_X^{m+n} e Def_{Xa}^m.

Referência: A Proposição 1.3.4 de [Marker], com outra numeração romana. O leitor pode considerar este um bom exercício para manipulação de fórmulas, de modo que faremos alguns breves comentários.

Para ver que a família $(\mathrm{Def}_A^m)_{m \in \mathbb{N}^*}$ tem essas propriedades é preciso escrever cada fórmula que defina os conjuntos envolvidos. Por exemplo: em (i), tome as fórmulas atômicas mais simples; em (iii), substitua previamente as variáveis livres comuns das fórmulas que definem D e E e tome sua conjunção. Se assumirmos que cada D_m é mínimo, temos $D_m \subseteq \mathrm{Def}_A^m$.

Para mostrar que $\mathrm{Def}_A^m \subseteq D_m$, considera-se $D = \phi(\mathfrak{A})$, em que ϕ é fórmula de L. Isso dá conta dos $\emptyset$-definíveis, bastando então aplicar (vi). Procede-se por indução na formação de ϕ e, inicialmente, na formação de um termo de L. Os casos atômicos ou desaninhados são verificados por (i) e (ii). Termos mais complexos requerem o uso das operações de (iv) e (v). Negações e conjunções são tratadas pela propriedade (iv) e a quantificação existencial por (v).

Verifica-se analogamente o

Corolário 1.3.5. Os conjuntos $\mathrm{Def}_\emptyset^m$ são os menores a satisfazerem essas propriedades com exceção de (vi). Todos os definíveis podem ser obtidos a partir de $\mathrm{Def}_{\emptyset}^{m}$ e aplicações de (vi).

Apresentamos agora a definição dos conceitos iniciais da Teoria dos Modelos com inspiração nesses resultados:

"Uma estrutura é um conjunto A acompanhado de álgebras de Boole $\mathrm{Def}_{\emptyset}^{m}$, subálgebra do conjunto das partes de A^m, contendo as diagonais e fechadas, como um todo, sob projeções e suas inversas. Os elementos dessas álgebras são chamados $\emptyset$-definíveis. Um subconjunto de A^m é chamado definível se é da forma $D_a = \{\alpha \in A^m \mid (\alpha, a) \in D\}$ para $D \in \mathrm{Def}_{\emptyset}^{m+n}$ e $a \in A^n$. Caso $X \subseteq A$ e $a \in X^n$, diz-se que D_a é X-definível. Uma subestrutura elementar de A é $B \subseteq A$ tal que, se $E \neq \emptyset$ é B-definível, então $E \cap B \neq \emptyset$. Consideramos então B uma estrutura cujos $\emptyset$-definíveis são as restrições a B dos $\emptyset$-definíveis de A."

Nesse contexto, pode-se definir uma nova linguagem tomando um predicado m-ário para cada elemento de $\mathrm{Def}_{\emptyset}^{m}$. Caso $\mathfrak{A}$ seja uma L-estrutura, a nova linguagem contém os predicados da linguagem obtida no Exemplo 1.1.3 e também inclui predicados equivalentes às fórmulas de L. Pela propriedade de fecho sob projeções e suas inversas, há naturalmente eliminação de quantificadores.

Considere agora uma função X-definível $f : R \to S$, em que $R \subseteq A^r$ e $S \subseteq A^s$. A imagem direta por f de um X-definível $D \subseteq A^r$ é X-definível,

$$f[D] = \{y \in S \mid \text{existe } x \in (R\cap)D \text{ tal que } f(x) = y\} ,$$

e a imagem inversa por f de um X-definível $E \subseteq A^s$ é X-definível,

$$f^{-1}[E] = \{x \in R \mid \text{existe } y \in (S\cap)E \text{ tal que } f(x) = y\} .$$

As fórmulas que definem f, D, E já bastam para escrever as novas fórmulas, mas R e S também são X-definíveis. Enfim, a composição de funções definíveis é uma função definível.

Notemos que todo subconjunto finito S de A^m é definível: de fato, é S-definível. Suponha que $S = \{s_1, \ldots, s_k\}$ em que $s_i = (s_{i1}, \ldots, s_{im})$. Então $\bigvee_{i=1}^{k} \bigwedge_{j=1}^{m} (v_j = s_{ij})$ define S. Assim, também é definível todo subconjunto cofinito, isto é, complemento de conjunto finito.

A coleção dos subconjuntos finitos e cofinitos de A é uma álgebra de Boole contida em Def_{A}^{1}. Quando contém realmente todos os definíveis de uma "coordenada", surgem propriedades importantes que encontraremos ao longo do texto, devendo-se isolar o conceito.

Um definível $D \in \mathrm{Def}_{A}^{m}$ é *minimal* se for infinito (hipótese simplificadora de caracterizações) e, para qualquer $E \in \mathrm{Def}_{A}^{m}$, ou $D \cap E$ ou $D - E$ é finito.

Porque D é infinito, o outro conjunto é forçosamente infinito. Veremos uma caracterização com posto de Morley "interno" na Proposição 2.1.15.

A estrutura $\mathfrak{A}$ é *minimal* se o definível $A \in \mathrm{Def}_A^1$ é minimal. Nesse caso, Def_A^1 é a álgebra dos subconjuntos finitos e cofinitos.

Uma fórmula ϕ de $\mathrm{L}(A)$ define um conjunto $\phi(\mathfrak{A})$ *fortemente minimal* se $\phi(\mathfrak{B})$ é minimal em toda extensão elementar $\mathfrak{B}$ de $\mathfrak{A}$. A caracterização com posto de Morley será apresentada na Proposição 2.1.21.

A estrutura $\mathfrak{A}$ é *fortemente minimal* se A é fortemente minimal, ou também, se toda extensão elementar de $\mathfrak{A}$ é minimal.

Finalmente, uma teoria é chamada *fortemente minimal* se todo modelo seu for fortemente minimal. Note que a situação é a mesma se supormos apenas que os modelos são minimais.

Exemplo 1.3.6. ACF é fortemente minimal. Para mostrá-lo, usemos a linguagem dos anéis com unidade. Em um corpo algebricamente fechado, que é infinito, toda fórmula equivale, por eliminação de quantificadores, a uma combinação booleana de fórmulas atômicas da forma "polinômio $= 0$", em que o polinômio tem coeficientes no corpo. Então todo definível com uma "coordenada" é combinação booleana de conjuntos de raízes de polinômios de uma variável, que são finitos ou todo o corpo (no caso do polinômio 0).

Esta caracterização dos conjuntos fortemente minimais é usada como definição em [Hrushovski, Zilber], por exemplo, e apresenta uma limitação uniforme para os conjuntos finitos de uma família uniformemente definível:

Proposição 1.3.7 (Uniformidade). Sejam $\mathfrak{A}$ uma L-estrutura e $D \in \mathrm{Def}_A^m$ *infinito.* Então D é fortemente minimal se e somente se, para cada fórmula $\phi(v, w)$ de L em que v, w são seqüências de m, n variáveis respectivamente, existe $k \in \mathbb{N}^*$ tal que $|D \cap \phi(\mathfrak{A}, a)| \leqslant k$ ou $|D - \phi(\mathfrak{A}, a)| \leqslant k$ para todo $a \in A^n$.

Demonstração: Escreva $D = \theta(\mathfrak{A})$ com $\theta(v)$ fórmula de $\mathrm{L}(A)$.

Suponha que D satisfaça a condição do enunciado e suponha $\mathfrak{B}$ uma extensão elementar de $\mathfrak{A}$. Temos

$$\mathfrak{A} \models \forall w \left(\exists^{\leqslant k} v\, (\theta(v) \wedge \phi(v, w)) \vee \exists^{\leqslant k} v\, (\theta(v) \wedge \neg\phi(v, w))\right) ,$$

de modo que também $\mathfrak{B}$ satisfaz essa sentença. Como ϕ é arbitrária e w pode ser interpretada por qualquer n-upla de elementos de B, concluímos que $\theta(\mathfrak{B})$ é minimal. Assim, D é fortemente minimal.

Assuma agora que D é fortemente minimal e ϕ como no enunciado, mas que para cada $k \in \mathbb{N}^*$ exista $a_k \in A^n$ com ambos os definíveis com mais de k elementos. Adicione a $\mathrm{L}(A)$ uma seqüência c de n novas constantes. Então

$$Th(\mathfrak{A}, (a)_{a\in A}) \cup \{\exists^{\geqslant k+1} v\,(\theta(v) \wedge \phi(v,c)) \wedge \exists^{\geqslant k+1} v\,(\theta(v) \wedge \neg\phi(v,c)) \mid k \in \mathbb{N}^*\}$$

é finitamente satisfazível, interpretando-se c como a_k em $\mathfrak{A}$, sendo k o limitante máximo das sentenças que ocorrerem em um subconjunto finito. Pelo Teorema da Compacidade, esse conjunto é uma teoria com um modelo que podemos supor $\mathfrak{B}$ extensão elementar de $\mathfrak{A}$ com c interpretada como $b \in B^n$. Desse modo, para qualquer $k \in \mathbb{N}^*$ temos $|\theta(\mathfrak{B}) \cap \phi(\mathfrak{B}, b)| > k$ ou $|\theta(\mathfrak{B}) - \phi(\mathfrak{B}, b)| > k$, contradizendo o fato de $\theta(\mathfrak{B})$ ser minimal. QED

Introduzimos agora os tipos, que mais estudaremos como ultrafiltros nas álgebras de definíveis.

Um *m-tipo sobre X* é um conjunto de fórmulas de $L(X)$ com m variáveis livres, usualmente identificadas $v_1, \ldots, v_m$, consistente com $Th(\mathfrak{A}, (x)_{x\in X})$ e maximal com respeito a inclusão. Indica-se um tipo como p ou $p(v)$.

Assim, todos os tipos são fechados sob conseqüência e conjunção e são *completos*, ou seja, contêm uma fórmula ou sua negação. É freqüente chamar qualquer conjunto consistente de fórmulas de tipo (parcial), mas não o faremos. Note também que os m-tipos sobre X correspondem a teorias completas em $L(X \cup \{c_1, \ldots, c_m\})$, sendo $c_1, \ldots, c_m$ são novas constantes, contendo $Th(\mathfrak{A}, (x)_{x\in X})$. Então o caso $m = 0$ é trivial, pois o único 0-tipo é $Th(\mathfrak{A}, (x)_{x\in X})$, e assumiremos sempre $m \geqslant 1$.

Indique $S_m^{\mathfrak{A}}(X)$ o conjunto dos m-tipos sobre X. Comecemos por desenvolver algum conhecimento a respeito desses conjuntos especiais de fórmulas.

Exemplo 1.3.8. Suponha L um corpo e K o subcorpo gerado por $X \subseteq L$. Vimos que uma fórmula com parâmetros em K reescreve-se equivalentemente como fórmula com parâmetros em X, de modo que a consistência e a maximalidade de um conjunto de fórmulas são sempre preservadas. Assim, identificaremos $S_m^L(K) = S_m^L(X)$. Ainda nesta seção, entenderemos os tipos como ultrafiltros da álgebra dos defíniveis. Como $\mathrm{Def}^m_{L,K} = \mathrm{Def}^m_{L,X}$, seus espaços de Stone são os mesmos.

Dado $a \in A^m$,

$$t_{\mathfrak{A}}(a/X) = \{\phi(v) \text{ de } L(X) \mid (\mathfrak{A}, (x)_{x\in X}) \models \phi(a)\}$$

é um tipo, chamado *principal de a*, porque é consistente (realizado por a) e maximal (contém uma fórmula ou sua negação). É o único (por maximalidade) realizado por a em $\mathfrak{A}$. (Escreve-se também $tp_{\mathfrak{A}}(a/X)$.) Pode-se indicar $t(a) = t(a/\emptyset)$.

Note que $t_{\mathfrak{A}}(a/X) = t_{\mathfrak{A}}(b/X)$ equivale a a e b satisfazerem as mesmas fórmulas de $L(X)$. O Exemplo 1.1.5, estendendo bijeções crescentes a automorfismos da ordem dos números reais, e a discussão na Seção 1.2, sobre elementos de corpos algebricamente fechados que são conjugados por automorfismos, sugerem a

Proposição 1.3.9. As m-uplas $a, b \in A^m$ têm o mesmo m-tipo sobre X se e somente se existem uma extensão elementar $\mathfrak{B}$ de $\mathfrak{A}$ e um automorfismo de $\mathfrak{B}$ sobre X que leva a a b.

Demonstração: Concentramo-nos em provar a implicação direta, porque a recíproca é imediata. Essa é a Proposição 4.1.5 de [Marker].

Procederemos em etapas. Suponha inicialmente $\mathfrak{C}, \mathfrak{D}$ quaisquer, $X \subseteq C$ e $f : X \to D$. Dizemos que f é *(parcial) elementar* se, para todas ϕ fórmula de L com n variáveis livres e $a \in X^n$, vale a equivalência $\mathfrak{C} \models \phi(a) \Leftrightarrow \mathfrak{D} \models \phi(f(a))$.

Provaremos inicialmente que, nas condições dessa definição e dado $x \in C$, existem uma extensão elementar $\mathfrak{D}_1$ de $\mathfrak{D}$ e uma função $g : X \cup \{x\} \to D_1$ elementar estendendo f. Adicione a $L(D)$ uma nova constante c e considere o conjunto de sentenças T constituído de $Th(\mathfrak{D}, (d)_{d \in D})$ e das sentenças $\phi(c, f(a))$ em que ϕ é formula de L com $n+1$ variáveis livres, $a \in C^n$ e $\mathfrak{C} \models \phi(x, a)$. O conjunto T é uma teoria pelo Teorema da Compacidade, porque é finitamente satisfazível: tomando conjunções, podemos trabalhar com uma única fórmula; se $\mathfrak{C} \models \phi(x, a)$ então $\mathfrak{C} \models \exists v\, \phi(v, a)$ e $\mathfrak{D} \models \exists v\, \phi(v, f(a))$ porque f é elementar, interpretando-se finalmente c como a interpretação de v. Podemos, como costumeiro, supor que o modelo $\mathfrak{D}_1$ de T é extensão elementar de $\mathfrak{D}$ com um elemento y interpretando a constante c. Basta então tomar $g(x) = y$; g é elementar pela definição de T.

Agora, ainda nessas condições, mostraremos como estender f a todo C, com imagem em uma extensão elementar de $\mathfrak{D}$. Note que então obteremos uma imersão elementar de $\mathfrak{C}$ na extensão de $\mathfrak{D}$. Indexe os elementos de C como x_ξ, $\xi < |C|$, e tome $\mathfrak{D}_0 = \mathfrak{D}$, $X_0 = X$ e $g_0 = f$. Escreva $X_\xi = X \cup \{x_\zeta \mid \zeta < \xi\}$. Definiremos indutivamente uma cadeia elementar $(\mathfrak{D}_\xi)_{\xi < |C|}$ e funções elementares $g_\xi : X_\xi \to D_\xi$ tais que $g_\xi|_{X_\zeta} = g_\zeta$ para $\zeta \leqslant \xi$. Já temos o caso $\xi = 0$. Se ξ é um ordinal sucessor, aplicamos o argumento anterior. Se ξ é um ordinal limite, tomamos $\mathfrak{D}_\xi = \bigcup_{\zeta < \xi} \mathfrak{D}_\zeta$ e g_ξ a colagem de todas as funções g_ζ, $\zeta < \xi$, que são compatíveis. Finalmente, $\bigcup_{\xi < |C|} \mathfrak{D}_\xi$ e a colagem g de todas as funções g_ξ são a extensão e a função que procurávamos.

Finalmente, retome as condições do enunciado. Tome $f : X \cup \{a\} \to A$ de $\mathfrak{A}$ a $\mathfrak{A}$ como a identidade em X e $f(a) = b$. Esta função está bem-definida e é elementar porque $t_{\mathfrak{A}}(a/X) = t_{\mathfrak{A}}(b/X)$. Escreva $\mathfrak{A}_0 = \mathfrak{A}$. Pelo último argumento, existem $\mathfrak{B}_0$ extensão elementar de $\mathfrak{A}_0$ e $f_0 : \mathfrak{A}_0 \to \mathfrak{B}_0$ imersão elementar estendendo f. Novamente procedendo por indução, acompanhe o diagrama a seguir. Dados $i \in \mathbb{N}$, $\mathfrak{A}_i \prec \mathfrak{B}_i$ e $f_i : \mathfrak{A}_i \to \mathfrak{B}_i$ imersão elementar, podemos ver $f_i^{-1} : f_i[A_i] \to B_i$ (já que $A_i \subseteq B_i$) como função elementar de $\mathfrak{B}_i$ a $\mathfrak{B}_i$. Também pelo último argumento, obtemos $\mathfrak{A}_{i+1}$ extensão elementar de $\mathfrak{B}_i$ e $g_i : \mathfrak{B}_i \to \mathfrak{A}_{i+1}$ imersão elementar estendendo f_i^{-1}. Mais uma vez, agora considerando $g_i^{-1} : g_i[B_i] \to A_{i+1}$ (já que $B_i \subseteq A_{i+1}$) elementar de $\mathfrak{A}_{i+1}$ a $\mathfrak{A}_{i+1}$, obtemos $\mathfrak{B}_{i+1}$ extensão elementar de $\mathfrak{A}_{i+1}$ e $f_{i+1} : \mathfrak{A}_{i+1} \to \mathfrak{B}_{i+1}$ imersão elementar estendendo g_i^{-1}. Desse modo, f_{i+1} estende f_i e B_i está contido na imagem de f_{i+1} porque é o domínio de g_i.

Este diagrama sumariza a construção, com flechas contínuas correspondendo a imersões elementares (sem rótulo quando são inclusões) e flechas pontilhadas a funções parciais elementares, cujos domínios são subconjuntos das estruturas indicadas:

$$\begin{tikzcd}
\mathfrak{B}_i \arrow[r] \arrow[drr, "g_i"] \arrow[dr, dotted, "f_i^{-1}"'] & \mathfrak{A}_{i+1} \arrow[r] & \mathfrak{B}_{i+1} \\
\mathfrak{A}_i \arrow[r] \arrow[u, "f_i"] & \mathfrak{B}_i \arrow[r] & \mathfrak{A}_{i+1} \arrow[u, "f_{i+1}"'] \arrow[ul, dotted, "g_i^{-1}"']
\end{tikzcd}$$

Obtemos as cadeias intercaladas

$$\mathfrak{A} = \mathfrak{A}_0 \prec \mathfrak{B}_0 \prec \mathfrak{A}_1 \prec \mathfrak{B}_1 \prec \mathfrak{A}_2 \prec \mathfrak{B}_2 \prec \mathfrak{A}_3 \prec \cdots$$

Sejam $\mathfrak{B} = \bigcup_{i \in \mathbb{N}} \mathfrak{A}_i$ e σ a colagem de todas as f_i, compatíveis. Note que também $\mathfrak{B} = \bigcup_{i \in \mathbb{N}} \mathfrak{B}_i$. Então $\mathfrak{A} \prec \mathfrak{B}$ e $\sigma : B \to B$ é uma função elementar com $\sigma|_X$ a identidade e $\sigma(a) = b$. Porque $B = \bigcup_{i \in \mathbb{N}} B_i$ e a imagem de f_{i+1} contém B_i, obtemos σ sobrejetora e, portanto, o automorfismo desejado. QED

Lema 1.3.10. Se $\Phi(v_1, \ldots, v_n)$ é um conjunto de fórmulas de $L(X)$ consistente com $Th(\mathfrak{A}, (x)_{x \in X})$, então Φ é consistente com toda $Th(\mathfrak{A}, (a)_{a \in A})$, de modo que existe uma extensão elementar de $\mathfrak{A}$ que realiza Φ. Em particular, todo tipo sobre X é consistente com $Th(\mathfrak{A}, (a)_{a \in A})$ e satisfeito em uma extensão elementar de $\mathfrak{A}$ e, por ser fechado sob conjunções, é finitamente satisfazível em $\mathfrak{A}$.

Demonstração: Esse enunciado contorna uma dificuldade: se $X \neq A$, um modelo de $Th(\mathfrak{A}, (x)_{x \in X})$ não precisa ser extensão elementar de $(\mathfrak{A}, (x)_{x \in X})$.

Substitua as variáveis de Φ por novas constantes, que indicaremos c, e tome $(\mathfrak{B}, (b_x)_{x \in X}, b)$ um modelo de $Th(\mathfrak{A}, (x)_{x \in X})$ que realiza $\Phi(c)$.

Pelo Teorema da Compacidade, basta mostrar que $\Phi(c) \cup Th(\mathfrak{A}, (a)_{a \in A})$ é finitamente satisfazível. Sejam Φ_0, T_0 subconjuntos finitos não-vazios de $\Phi(\mathfrak{C})$,

$Th(\mathfrak{A}, (a)_{a\in A})$ respectivamente. Substitua por novas variáveis v as constantes de $A - X$ nas sentenças de T_0 e seja $\phi(v)$ a conjunção em $L(X)$ das fórmulas obtidas. Portanto, $\exists v\, \phi(v) \in Th(\mathfrak{A}, (x)_{x\in X})$. Seja σ a conjunção das sentenças de Φ_0: trata-se de uma sentença com constantes em X e as novas c; vemos que σ é conseqüência de $\Phi(c)$.

Então $(\mathfrak{B}, (b_x)_{x\in X}, b) \models \sigma \wedge \exists v\, \phi(v)$. Interpretando as constantes de $A - X$ como os elementos que satisfazem ϕ, vemos que $\Phi_0 \cup T_0$ tem um modelo. QED

Corolário 1.3.11. Se $\mathfrak{A} \prec \mathfrak{B}$ então $S_m^{\mathfrak{A}}(X) = S_m^{\mathfrak{B}}(X)$ e $t_{\mathfrak{A}}(a/X) = t_{\mathfrak{B}}(a/X)$.

Demonstração: Observe que $Th(\mathfrak{A}, (x)_{x\in X}) = Th(\mathfrak{B}, (x)_{x\in X})$ e a linguagem continua sendo $L(X)$, de modo que a condição de consistência e maximalidade é a mesma quanto a $\mathfrak{A}$ ou $\mathfrak{B}$.

Como $(\mathfrak{A}, (x)_{x\in X}) \prec (\mathfrak{B}, (x)_{x\in X})$, o tipo de a é também o mesmo. QED

Desse modo, todo conjunto de fórmulas $\Phi(v_1, \ldots, v_m)$ de $L(X)$ consistente com $Th(\mathfrak{A}, (x)_{x\in X})$ estende-se a um tipo sobre X. De fato, Φ é consistente com $Th(\mathfrak{A}, (a)_{a\in A})$, existindo então $\mathfrak{A} \prec \mathfrak{B}$ e $b \in B^m$ tais que $(\mathfrak{B}, (a)_{a\in A}) \models \Phi(b)$. Assim, $\Phi \subseteq t_{\mathfrak{B}}(b/X) \in S_m^{\mathfrak{A}}(X)$. Um outro modo de estender Φ é substituir as variáveis por novas constantes e unir com $Th(\mathfrak{A}, (x)_{x\in X})$, obtendo uma teoria a que se aplica o Teorema de Lindenbaum.

Corolário 1.3.12. $S_m^{\mathfrak{A}}(X)$ é o conjunto dos tipos $t_{\mathfrak{B}}(b/X)$ em que $\mathfrak{B}$ é uma extensão elementar de $\mathfrak{A}$ e $b \in B^m$.

Demonstração: Se $\mathfrak{B}$ é uma extensão elementar de $\mathfrak{A}$ e $b \in B^m$, então $t_{\mathfrak{B}}(b/X) \in S_m^{\mathfrak{B}}(X) = S_m^{\mathfrak{A}}(X)$.

Suponha então $p \in S_m^{\mathfrak{A}}(X)$. Pelo lema, existem uma extensão elementar $\mathfrak{B}$ de $\mathfrak{A}$ e $b \in B^m$ que realiza p. Por unicidade, $p = t_{\mathfrak{B}}(b/X)$. Concluímos que $p \in S_m^{\mathfrak{B}}(X)$.

Podemos tomar uma única extensão $\mathfrak{B}$ para todos os m-tipos. Enumere-os p_ξ, $\xi < |S_m^{\mathfrak{A}}(X)|$, sem repetição. Por indução, suponha definida uma cadeia elementar $(\mathfrak{B}_\zeta)_{\zeta<\xi}$ para $\xi < |S_m^{\mathfrak{A}}(X)|$, com $\mathfrak{A} \prec \mathfrak{B}_0$ e cada $\mathfrak{B}_\zeta$ realizando p_ζ. Tome $\mathfrak{B}_\xi$ uma extensão elementar de $\bigcup_{\zeta<\xi} \mathfrak{B}_\zeta$ que realize p_ξ. Então $\mathfrak{B} = \bigcup_{\xi<|S_m^{\mathfrak{A}}(X)|} \mathfrak{B}_\xi$ é uma extensão elementar de $\mathfrak{A}$ que realiza todos os tipos de $S_m^{\mathfrak{A}}(X)$.

Do mesmo modo, podemos tomar uma única extensão $\mathfrak{B}$ para todos os tipos sobre X. QED

Exemplo 1.3.13. Para estudar $S_1^{\mathbb{Q}}(\mathbb{Q})$ na linguagem das ordens, é conveniente já trabalhar em uma extensão elementar de $\mathbb{Q}$ em que todos os 1-tipos sejam realizados. Não construiremos essa extensão: o leitor pode servir-se de um modelo de Análise Não-*Standard* (veja nossas referências básicas) ou construir uma ultrapotência de $\mathbb{Q}$.

A cardinalidade máxima de $S_1^{\mathbb{Q}}(\mathbb{Q})$ é 2^ω, porque a linguagem das ordens com parâmetros em $\mathbb{Q}$ é enumerável, sendo portanto enumerável o conjunto de suas fórmulas de uma variável, e cada elemento de $S_1^{\mathbb{Q}}(\mathbb{Q})$ é um subconjunto desse conjunto. Mostremos que o máximo é realmente atingido.

Como $\mathbb{Q} \prec \mathbb{R}$ nessa linguagem, cada $x \in \mathbb{R}$ define um tipo $t_{\mathbb{Q}}(x/\mathbb{Q})(v)$, que contém as fórmulas $r < v$ para todo racional $r < x$. Essa associação é injetora e produz portanto $|\mathbb{R}|$ tipos. Assim, $|S_1^{\mathbb{Q}}(\mathbb{Q})| = 2^\omega$. Dentre esses tipos $t_{\mathbb{Q}}(x/\mathbb{Q})$, há duas espécies: quando x é racional e o tipo é realizado em $\mathbb{Q}$, e quando x é irracional e o tipo não é realizado em $\mathbb{Q}$.

Fixado $r \in \mathbb{Q}$, também podemos considerar um elemento infinitesimalmente maior que r, ou seja, um elemento x de uma extensão elementar tal que $r < x$ e todo racional maior que r é maior que x. Evidentemente, x não pode ser real, mas os elementos que devem existir entre r e x para que a ordem seja densa também não precisam ser racionais. Desse modo, x e qualquer outro elemento entre r e os racionais $> r$ são conjugados por um automorfismo de ordem sobre $\mathbb{Q}$. O tipo de x sobre $\mathbb{Q}$ é o único de todos esses elementos e pode ser indicado r^+. Analogamente, existe o tipo r^-.

Existem também extensões elementares de $\mathbb{Q}$ e $\mathbb{R}$ que, embora não tenham um último elemento, têm elementos maiores que todos os racionais e os reais. Como a ordem é densa e os elementos superam todos os racionais, quaisquer dois desses elementos são conjugados por um automorfismo de ordem sobre $\mathbb{Q}$. Assim, o tipo desses elementos sobre $\mathbb{Q}$ é único e pode ser indicado $+\infty$. Analogamente, existe o tipo $-\infty$.

A argumentação com automorfismos de ordem também mostra que esses tipos são todos distintos e essas são todas as possibilidades de posição entre os racionais e um elemento em uma extensão elementar. O mesmo estudo aplica-se a qualquer ordem linear, densa e sem extremidades.

Não será necessário indicarmos, na maioria das situações, com que estrutura trabalhamos. Assim, escreveremos apenas $S_m(X)$ e $t(a/X)$. Convém também indicar $S(X) = \bigcup_{m \in \mathbb{N}^*} S_m(X)$.

Procedemos agora à identificação de tipos com ultrafiltros, o que facilitará nosso trabalho. A um subconjunto $U \subseteq \mathrm{Def}_X^m$ associa-se naturalmente, como vimos, o conjunto U' de *todas* as fórmulas de $\mathrm{L}(X)$ com variáveis livres dentre $v_1, \ldots, v_m$ que definem os elementos de U. Obtemos esta caracterização dos tipos, de que faremos uso freqüente:

Proposição 1.3.14. (i) Se U é um ultrafiltro em Def_X^m então U' é um m-tipo.

(ii) Se $p \in S_m^{\mathfrak{A}}(X)$, então $U = \{D \in \mathrm{Def}_X^m \mid D = \phi(\mathfrak{A}, (x)_{x \in X})$ e $\phi \in p\}$ é um ultrafiltro em Def_X^m e $U' = p$.

Demonstração: Para provar (i), suponha que U é um ultrafiltro. Como U é filtro próprio, tem a propriedade da intersecção finita. Então U' é consistente com $Th(\mathfrak{A}, (x)_{x \in X})$ pelo Corolário 1.3.3. Suponha que $\phi(v)$ fórmula de $\mathrm{L}(X)$ não pertença a U', de modo que $\phi(\mathfrak{A}, (x)_{x \in X}) \notin U$ e então $(\neg\phi)(\mathfrak{A}, (x)_{x \in X}) \in U$, donde $\neg\phi \in U'$. Então U' é maximal, pois qualquer conjunto que o contenha propriamente contém uma fórmula e sua negação, não sendo consistente.

Quanto a (ii), assuma que p é um tipo. Como é maximal, é fechado sob conjunções e conseqüências, de modo que U é um filtro. U é próprio pois p é consistente com $Th(\mathfrak{A}, (x)_{x \in X})$: há um modelo dessa teoria que realiza p; como ela é completa, se $\phi \in p$ então $Th(\mathfrak{A}, (x)_{x \in X}) \models \exists v\, \phi(v)$, donde $\phi(\mathfrak{A}, (x)_{x \in X}) \neq \emptyset$. U é maximal, pois se V é um ultrafiltro que contém U então V' é um tipo por (i) e contém p maximal, donde $V' = p$ e $U = V$. Concluímos também que $U' = p$.

QED

Ou seja: um conjunto de fórmulas com número finito de variáveis livres é um tipo se e somente se, em sua linguagem, é fechado sob conjunções, conseqüências e contém uma fórmula se e somente se não contém sua negação.

Exemplo 1.3.15. Suponha $p \in S_m(X)$ e σ um automorfismo de $\mathfrak{A}$. Defina $\sigma \cdot p$ como o conjunto das fórmulas $\phi(v, \sigma(x))$ em que $\phi(v, w)$ é fórmula de L e x é uma seqüência apropriada de elementos de X tais que $\phi(v, x) \in p(v)$. Pela caracterização por ultrafiltro, vemos que $\sigma \cdot p$ é um tipo sobre $\sigma[X]$. Verifica-se que a operação $\cdot$ é uma ação do grupo dos automorfismos de $\mathfrak{A}$ sobre o conjunto dos tipos sobre subconjuntos de A. Em particular, quando $X = A$, o grupo dos automorfismos age sobre o espaço $S_m(A)$. Diz-se que σ *fixa* p se $\sigma \cdot p = p$.

Cuidado: se $\mathfrak{A} \prec \mathfrak{B}$, vimos que $S_m^{\mathfrak{A}}(X) = S_m^{\mathfrak{B}}(X)$. Enquanto conjuntos de fórmulas, os tipos são os mesmos, mas não enquanto ultrafiltros: $\mathrm{Def}_{\mathfrak{A},X}^m \neq \mathrm{Def}_{\mathfrak{B},X}^m$, já que os definíveis ganham novos elementos.

Vemos que a associação $(\cdot)'$ é injetora, e o item (ii) mostra que é sobrejetora. Assim, o conjunto $S_m(X)$ dos m-tipos sobre X identifica-se com o próprio *espaço de Stone* de Def_X^m. Note ainda que $t(a/X)$ identifica-se com $\{D \in \mathrm{Def}_X^m | a \in D\}$.

Corolário 1.3.16. Se ainda U for principal, então $U' = t(a/X)$ para algum $a \in A^m$, de modo recíproco se $a \in X^m$.

Demonstração: Se U é principal, é gerado por $D \in \mathrm{Def}_X^m$ não-vazio: tome $a \in D$ qualquer. Então $U' \subseteq t(a/X)$, mas temos a igualdade por U' ser maximal. Reciprocamente, se $a_1, \ldots, a_m \in X$, então a é X-definível e U é gerado por $\{a\}$.

QED

Em particular, a correspondência mostra-se completa quando $X = A$, caso em que se diz que os tipos são *globais*, também simplesmente chamados *sobre modelo(s)*. Afinal, todo definível é A-definível, de modo que a álgebra Def_A^m tem importância destacada. Veremos, ao longo do texto, que muitas propriedades escrevem-se mais facilmente para tipos globais.

É preciso compreender também, para $X \subseteq Y \subseteq A$ e $p \in S_m(X)$, $q \in S_m(Y)$, a inclusão $p \subseteq q$, quando se diz que q é *extensão* de p. Como conjunto de fórmulas de $\mathrm{L}(Y)$ ou de definíveis de Def_Y^m, p é ainda um filtro contido em q. Por maximalidade, é claro que $p = q$ se $X = Y$.

Indicamos $q|_X$ o conjunto das fórmulas de q que são da linguagem $\mathrm{L}(X)$, ou seja, $q|_X = \{D \in \mathrm{Def}_X^m \mid D \in q\}$. Observamos que $q|_X$ é um tipo sobre X, porque os fatos de q ser ultrafiltro e Def_X^m ser subálgebra de Def_Y^m tornam $q|_X$ um ultrafiltro também. Temos $p \subseteq q|_X$, donde $p = q|_X$ por maximalidade: então $q|_X$ é o único tipo sobre X contido em q.

Desse modo, $t(a/Y)|_X = t(a/X)$ pois $t(a/X) \subseteq t(a/Y)$.

Daremos agora uma topologia ao espaço $S_m(X)$ e, para conveniência, resumiremos algumas propriedades.

Tomamos, como abertos básicos de $S_m(X)$, estes conjuntos: para $D \in \mathrm{Def}_X^m$,

$$\langle D \rangle = \{p \in S_m(X) \mid D \in p\} .$$

Antes mesmo de verificar que esses conjuntos formam uma base, recordamos o

Fato 1.3.17. Para $D, E \in \mathrm{Def}_X^m$, valem:

(i) $\langle A^m \rangle = S_m(X)$ e $\langle \emptyset \rangle = \emptyset$.

(ii) $\langle D \cup E \rangle = \langle D \rangle \cup \langle E \rangle$; $\langle D \cap E \rangle = \langle D \rangle \cap \langle E \rangle$ e $\langle D - E \rangle = \langle D \rangle - \langle E \rangle$.

(iii) $\langle D \rangle \subseteq \langle E \rangle \Leftrightarrow D \subseteq E$.

Estas são regras básicas que valem no espaço de Stone de qualquer álgebra de Boole, observando-se que $\langle \cdot \rangle$ é um isomorfismo dessas álgebras. Também podem ser verificadas diretamente. Por exemplo, demonstremos a afirmação (iii). Se $D \subseteq E$, por definição todo ultrafiltro que contenha D contém E e vem $\langle D \rangle \subseteq \langle E \rangle$. Se $\langle D \rangle \subseteq \langle E \rangle$, então todo ultrafiltro que contenha D contém E. Não existe, portanto, ultrafiltro que contenha D e $A^m - E$, de modo que $D \cap (A^m - E) = \emptyset$ — caso contrário, seria uma família com a propriedade da intersecção finita. Assim, $D \subseteq E$.

Agora, é fácil verificar que a família $\{\langle D \rangle \mid D \in \mathrm{Def}_X^m\}$ é uma base topológica. Suponha $p \in S_m(X)$. Como $p \neq \emptyset$, existe $D \in p$, de modo que $p \in \langle D \rangle$. Caso

$p \in \langle D \rangle \cap \langle E \rangle$, temos $p \in \langle D \cap E \rangle \subseteq \langle D \rangle \cap \langle E \rangle$, como desejado. Vemos ainda que essa base é de abertos que são fechados, chamados *clopen* em inglês.

Se $\mathfrak{A} \prec \mathfrak{B}$, a topologia de $S_m^{\mathfrak{B}}(X)$ é a mesma de $S_m^{\mathfrak{A}}(X)$, porque as classes de fórmulas equivalentes são as mesmas.

Vemos, por exemplo, que para $X \subseteq Y \subseteq A$ a função que leva $q \in S_m(Y)$ a $q|_X \in S_m(X)$ é contínua. Afinal, para um X-definível D, vale $q|_X \in \langle D \rangle$ se e somente se $q \in \langle D \rangle$, sendo aqui D como Y-definível, já que $q|_X \subseteq q$.

Os pontos isolados são tipos principais. Se $p \in S(X)$ é isolado por $\langle D \rangle$, então $D \in p$ e $D \neq \emptyset$. Tomando $a \in D$, obtemos $D \in t(a/X)$ e $t(a/X) \in \langle D \rangle = \{p\}$, como desejado. A recíproca vale, novamente, quando $X = A$, porque $t(a/A)$ é isolado por $\langle \{a\} \rangle$, já que a é A-definível.

Esse raciocínio também mostra que os tipos principais formam um conjunto denso em seu espaço.

Proposição 1.3.18. Com essa topologia, $S_m(X)$ é um espaço compacto Hausdorff (ou T_2) totalmente desconexo, isto é, em que cada componente conexa contém apenas um ponto.

Demonstração: Novamente, trata-se de um resultado com demonstração comum aos espaços de Stone de todas as álgebras de Boole.

Começamos com a propriedade de Hausdorff. Suponha $p, q \in S_m(X)$ distintos. Por maximalidade, então p não está contido em q, existindo $D \in p$ com $D \notin q$, ou seja, $A^m - D \in q$. Assim, $p \in \langle D \rangle$ e $q \in \langle A^m - D \rangle$, que sabemos serem abertos disjuntos.

A propriedade de compacidade precisa ser verificada apenas em coberturas por abertos básicos. Suponha que $S_m(X) = \bigcup_{i \in I} \langle D_i \rangle$ sem subcobertura finita. Para todo subconjunto finito I_0 de I, temos $\langle \bigcup_{i \in I_0} D_i \rangle \neq S_m(X)$, donde $\bigcap_{i \in I_0} (A^m - D_i) \neq \emptyset$. Concluímos que $\{A^m - D_i \mid i \in I\}$ tem a propriedade da intersecção finita, estando contido em um ultrafiltro $p \in S_m(X)$. Mas $p \in \bigcup_{i \in I} \langle D_i \rangle$, de modo que existe $i \in I$ com $D_i \in p$, contradizendo $A^m - D_i \in p$.

Finalmente, se p, q são pontos distintos de um conjunto $R \subseteq S_m(X)$, vimos que existe um aberto básico $\langle D \rangle$ que contém p, mas não q. Então $q \in \langle A^m - D \rangle$ e $R = (R \cap \langle D \rangle) \cup (R \cap \langle A^m - D \rangle)$ mostra que R é desconexo. QED

Por exemplo, a compacidade implica que um *clopen* é união *finita* de abertos básicos e, portanto, já pertence a essa família, que é uma álgebra de Boole.

Exemplo 1.3.19. Suponha L um corpo algebricamente fechado e K um subcorpo qualquer de L. Estudemos o espaço $S_1^L(K)$.

Se $a \in L$ é algébrico sobre K, mostraremos que o tipo $t(a/K)$ é isolado pelo aberto básico correspondente ao conjunto K-definível das raízes do polinômio minimal de a sobre K. Sejam p um tipo sobre K nesse aberto e L' uma extensão elementar de L com $b \in L'$ realizando p. Por definição, b é raiz do polinômio minimal de a sobre K. Ambos a e b anulam apenas os polinômios que são divisíveis por seu polinômio minimal e, portanto, anulam precisamente os mesmos termos de uma variável com parâmetros em K. Sabemos que, assim, a e b satisfazem precisamente as mesmas fórmulas atômicas de uma variável livre com parâmetros em K e, por combinação booleana, as mesmas fórmulas sem quantificadores de uma variável livre. Mas ACF admite eliminação de quantificadores, permitindo-nos concluir que a e b satisfazem as mesmas fórmulas de uma variável livre com parâmetros em $K \subseteq L$. Assim, $p = t(a/K)$ e quaisquer duas raízes do mesmo polinômio irredutível têm o mesmo tipo.

Se $a, b \in L$ são dois transcendentes sobre K, ambos anulam apenas o polinômio 0 dentre aqueles com coeficientes em K. Novamente, a e b satisfazem as mesmas fórmulas de uma variável livre com parâmetros em K. Assim, $t(a/K) = t(b/K)$, um único tipo chamado *dos transcendentes*, que vemos não ser de nenhum algébrico. Mesmo que não existam elementos de L transcendentes sobre K, esse tipo existe: o mesmo raciocínio mostra que é o tipo de um elemento transcendente sobre K em uma extensão elementar de L.

Sabemos que o fecho algébrico de K em L é infinito, porque L é algebricamente fechado. Como cada polinômio minimal sobre K tem um número finito de raízes, esses polinômios são em número infinito e, portanto, $S_1(K)$ é infinito. Já que $S_1(K)$ é compacto, tem um ponto de acumulação, necessariamente o tipo dos elementos transcendentes. Concluímos uma caracterização topológica de $S_1(K)$.

Exemplo 1.3.20 (Espaço espectral). Suponha ainda $K \subseteq L$ corpos, com L algebricamente fechado. Trabalharemos com o espaço $S^L_m(K)$ e também com o conjunto $\operatorname{Spec} K[x_1, \ldots, x_m]$ dos ideias primos *próprios* de $K[x_1, \ldots, x_m]$. Esse conjunto pode ser definido para qualquer anel R e tem uma topologia chamada *espectral ou de Zariski* com fechados básicos $\{P \in \operatorname{Spec} R \mid r \in P\}$, $r \in R$.

Para $P, Q \in \operatorname{Spec} R$, vale então a curiosa propriedade de que Q pertence ao fecho de $\{P\}$ se e somente se $P \subseteq Q$. Portanto, o ideal $\{0\}$ é um *ponto genérico* de $\operatorname{Spec} K[x_1, \ldots, x_m]$: seu unitário é denso no espaço (mostra-se que qualquer $\operatorname{Spec} R$ tem um ponto genérico; é o ideal dos elementos nilpotentes se for primo).

Dado $p \in S_m(K)$, considere o conjunto $\varphi(p)$ dos polinômios $f \in K[x_1, \ldots, x_m]$ tais que a fórmula $f(v) = 0$ esteja em p. Verifica-se que $\varphi(p)$ é um ideal primo do anel $K[x_1, \ldots, x_m]$, próprio porque o polinômio constante 1 não pode pertencer a $\varphi(p)$ ($1 = 0$ não é consistente com o diagrama elementar de L). Obtemos uma função $\varphi : S_m(K) \to \operatorname{Spec} K[x_1, \ldots, x_m]$.

Por exemplo, quando $m = 1$, a imagem por φ do tipo dos elementos transcendentes é o ideal $\{0\}$.

Para ver que φ é injetora, suponha $p, q \in S_m(K)$ com $\varphi(p) = \varphi(q)$. Dada uma fórmula $\phi(v_1, \ldots, v_m)$ com parâmetros em K, por eliminação de quantificadores ϕ é combinação booleana de fórmulas atômicas que correspondem a polinômios de $K[x_1, \ldots, x_m]$ igualados a 0. Já que $\varphi(p) = \varphi(q)$, as fórmulas dentre estas que estão em p são precisamente as que estão em q, de modo que também $\phi \in p \Leftrightarrow \phi \in q$ quando usamos a caracterização mencionada após a Proposição 1.3.14. Assim, $p = q$.

Mostremos que φ é também sobrejetora. Dado um ideal primo próprio P de $K[x_1, \ldots, x_m]$, pode-se mostrar que $P = Q \cap K[x_1, \ldots, x_m]$ para Q ideal primo próprio de $L[x_1, \ldots, x_m]$. Seja F um fecho algébrico do corpo de frações de $L[x_1, \ldots, x_m]/Q$: podemos assumir $L \subseteq F$ e então $L \prec F$. Sendo $t_i \in F$ correspondente a x_i/Q, para $f \in K[x_1, \ldots, x_m]$ temos $f(t_1, \ldots, t_m) = 0 \Leftrightarrow f \in Q$, de modo que $\varphi(t_F((t_1, \ldots, t_m)/K)) = P$.

Finalmente, φ é contínua. De fato, dado $f \in K[x_1, \ldots, x_m]$, a imagem inversa de $\{P \in \operatorname{Spec} K[x_1, \ldots, x_m] \mid f \in P\}$ é $\{p \in S_m(K) \mid (f(v) = 0) \in p(v)\}$ o *clopen* básico do conjunto definível das raízes de f. Porém, φ ***não*** é um homeomorfismo, pois se fosse então $S_m^L(K)$ teria um ponto genérico, contradizendo sua propriedade Hausdorff. Contudo, podemos concluir que $\operatorname{Spec} K[x_1, \ldots, x_m]$ é compacto.

Pelo Teorema da Base de Hilbert (veja enunciado e referências no Teorema 6.1.4), todo ideal em $K[x_1, \ldots, x_m]$ é finitamente gerado. Desse modo, existem até $\max\{|K|, \omega\}$ ideais em $K[x_1, \ldots, x_m]$. Por outro lado, o último parágrafo do exemplo anterior permite-nos calcular $|S_1(K)| \geqslant \omega, |K|$. Ao estender 1-tipos a m-tipos, porque são consistentes independentemente do número de variáveis, obtemos uma injeção em $S_m(K)$. Concluímos que $|S_m^L(K)| = |K| + \omega$.

1.4. O modelo monstro

Introduzimos algumas importantes propriedades, devidas a Morley e Vaught, Shelah (homogeneidade forte) e Hodges (grandeza). Nosso objetivo último é mostrar que existem estruturas com essas propriedades, mas previamente derivaremos caracterizações.

Observamos que, em alguns textos, há diferenças sutis nas definições, permutando as desigualdades $<$ e $\leqslant$.

Considere um cardinal infinito κ e uma L-estrutura $\mathfrak{A}$.

$\mathfrak{A}$ é *κ-saturada* se, para todo $X \subseteq A$ com $|X| < \kappa$, todo tipo de $S(X)$ é satisfazível em $(\mathfrak{A}, (x)_{x \in X})$ e, portanto, principal. $\mathfrak{A}$ é *saturada* se for $|A|$-saturada.

É suficiente verificar a condição para 1-tipos porque se procede por indução. De fato, dado um tipo $p(v_1, \ldots, v_m)$ sobre X com $m > 1$, podemos considerar o conjunto consistente de fórmulas contidas em p com apenas as variáveis livres $v_1, \ldots, v_{m-1}$. Esse conjunto estende-se a um $(m-1)$-tipo, que se assume realizado por $a \in A^{m-1}$. Desse modo, basta realizar $p(a, v_m)$ sobre Xa e, porque κ é infinito, temos $|Xa| \leqslant |X| + m - 1 < \kappa$.

Em algumas ocasiões, substituiremos κ por um cardinal finito, mas é simplesmente questão de abreviatura que pode ser expandida a um enunciado coerente. É o caso da $|A|$-saturação. Desejaríamos obter até $|A|^+$-saturação, para que os tipos globais de $S(A)$ também fossem principais, entretanto se verificaria que $|A| < \omega$, porque podemos considerar o conjunto de fórmulas $v \neq a$, $a \in A$. Reciprocamente, toda estrutura finita é saturada. Observamos, com isso, que os conceitos que introduziremos só se aproximam de nossa expectativa intuitiva quando aplicados a estruturas infinitas.

Exemplo 1.4.1. Um corpo algebricamente fechado L é saturado se tem grau de transcendência infinito sobre seu subcorpo primo. Em particular, todo corpo algebricamente fechado não-enumerável, como $\mathbb{C}$, é saturado.

Trabalharemos com 1-tipos. Suponha $X \subseteq L$ com $|X| < |L|$ e $p \in S_1^L(X)$. Seja K o subcorpo de L gerado por X. Existem $L \prec L'$ e $b \in L'$ que realiza p. Se b é algébrico sobre K então $b \in L$, como desejado. Se b é transcendente sobre K, tome $a \in L$ transcendente sobre K — de fato existe, porque $|L|$ é o grau de transcendência de L sobre seu subcorpo primo L_0, digamos, e $|X| < |L|$, de modo que $|K| = |L_0(X)| < |L|$ e o fecho algébrico de K em L tem cardinalidade $|K| \times \omega < |L|$. Temos $a, b \in L'$ transcendentes sobre K, de modo que existe um automorfismo σ de L' sobre K com $\sigma(a) = b$. Como $p \in S_1^{L'}(X)$ e $L' \models p(b)$, temos $L' \models p(a)$, de modo que $a \in L$ realiza p.

Este é um resultado de uso freqüente:

Proposição 1.4.2. Destas condições, cada uma implica a subseqüente, e equivalem para $\kappa > |\mathrm{L}|$:

(i) $\mathfrak{A}$ é κ-saturada.

(ii) Suponha $X \subseteq A$ com $|X| < \kappa$. Então qualquer conjunto de fórmulas de $\mathrm{L}(X)$ com número finito de variáveis livres que seja realizado em uma extensão elementar de $(\mathfrak{A}, (x)_{x \in X})$ é realizado em $(\mathfrak{A}, (x)_{x \in X})$.

(iii) Suponha $X \subseteq A$ com $|X| < \kappa$. Então qualquer conjunto de fórmulas de $\mathrm{L}(X)$ com número finito de variáveis livres que seja finitamente satisfazível em $(\mathfrak{A}, (x)_{x \in X})$ é realizado em $(\mathfrak{A}, (x)_{x \in X})$.

(iv) Se D_ξ, $\xi < \kappa$, são uma família de subconjuntos definíveis de A^m com a propriedade da intersecção finita, então $\bigcap_{\xi<\kappa} D_\xi \neq \emptyset$. Com esta propriedade, diz-se que $\mathfrak{A}$ é *κ-compacta*.

Demonstração: Observamos que, na condição (ii), a elementaridade da extensão é essencial, como se deduz do Exemplo 1.1.8. Para $\kappa = |\mathrm{L}| = \omega$, vê-se que (iv) não implica (i).

(i) $\Rightarrow$ (ii): Um tal conjunto Φ é consistente com $Th(\mathfrak{A}, (x)_{x \in X})$ por definição e estende-se a um tipo de $S(X)$. A κ-saturação de $\mathfrak{A}$ implica que esse tipo é realizado em $(\mathfrak{A}, (x)_{x \in X})$, de modo que Φ também.

(ii) $\Rightarrow$ (iii): Basta aplicar o Corolário 1.1.12.

(iii) $\Rightarrow$ (iv): Note que os parâmetros das fórmulas que definem os conjuntos D_ξ formam um conjunto de cardinal $< \kappa$. A propriedade da intersecção finita corresponde à satisfação finita dessa família de fórmulas, cuja realização por sua vez corresponde à intersecção não-vazia.

(iv) $\Rightarrow$ (i): Considere $X \subseteq A$ com $|X| < \kappa$ e $p \in S_m(X)$ como ultrafiltro de Def^m_X. Então seus definíveis têm a propriedade da intersecção finita. Como $|p| \leqslant |\mathrm{L}(X)| < \kappa$, tais conjuntos têm intersecção comum; concluímos que p é satisfazível em $(\mathfrak{A}, (x)_{x \in X})$. QED

Lema 1.4.3. A condição de $\mathfrak{A}$ ser κ-saturada equivale a este enunciado: "Sejam $\mathfrak{B}$ uma L-estrutura qualquer, $X \subseteq A$ e $Y \subseteq B$ com $|X| = |Y| < \kappa$ e $b \in B$. Se $(\mathfrak{A}, (x)_{x \in X}) \equiv (\mathfrak{B}, (y)_{y \in Y})$, em que se entende fixada uma correspondência biunívoca entre as constantes de X e Y, então existe $a \in A$ tal que $(\mathfrak{A}, (x)_{x \in X}, a) \equiv (\mathfrak{B}, (y)_{y \in Y}, b)$."

Demonstração: Assuma $\mathfrak{A}$ κ-saturada e a situação do enunciado. O tipo $t(b/Y)$ é um conjunto de fórmulas de $\mathrm{L}(X)$, quando as constantes de Y são substituídas pelas correspondentes de X, consistente com $Th(\mathfrak{A}, (x)_{x \in X})$ por ser finitamente satisfazível via quantificação existencial. Estende-se portanto a um tipo sobre X, realizado por $a \in A$. As sentenças de $\mathrm{L}(Yb)$ correspondem a fórmulas de $\mathrm{L}(Y)$ com parâmetro b e então a fórmulas de $\mathrm{L}(X)$ com parâmetro a, implicando a equivalência elementar desejada.

Assuma então o enunciado e suponha $p \in S_m(X)$. Existem então uma extensão elementar $\mathfrak{B}$ de $\mathfrak{A}$ e $(b_1, \dots, b_m) \in B^m$ tais que $p = t((b_1, \dots, b_m)/X)$. Como $(\mathfrak{A}, (x)_{x \in X}) \equiv (\mathfrak{B}, (x)_{x \in X})$, existe $a_1 \in A$ tal que $(\mathfrak{A}, (x)_{x \in X}, a_1) \equiv (\mathfrak{B}, (x)_{x \in X}, b_1)$. Temos $|Xa_1| = |Yb_1| < \kappa$, sendo κ infinito e a igualdade garantida pela equivalência elementar. Então obtemos $a_2 \in A$ correspondendo a b_2 e, sucessivamente, até

$$(\mathfrak{A}, (x)_{x\in X}, a_1, \ldots, a_m) \equiv (\mathfrak{B}, (x)_{x\in X}, b_1, \ldots, b_m)\,.$$

Portanto, $(a_1, \ldots, a_m)$ realiza p em $(\mathfrak{A}, (x)_{x\in X})$. QED

$\mathfrak{A}$ é *κ-universal* se toda L-estrutura elementarmente equivalente a $\mathfrak{A}$ e de cardinal $< \kappa$ pode ser elementarmente imersa em $\mathfrak{A}$.

$\mathfrak{A}$ é *κ-homogênea* se, para todos $X, Y \subseteq A$ com $|X| = |Y| < \kappa$ tais que $(\mathfrak{A}, (x)_{x\in X}) \equiv (\mathfrak{A}, (y)_{y\in Y})$, em que se entende fixada uma correspondência biunívoca entre as constantes de X e Y, e dado $a \in A$, existe $b \in A$ tal que $(\mathfrak{A}, (x)_{x\in X}, a) \equiv (\mathfrak{A}, (y)_{y\in Y}, b)$.

$\mathfrak{A}$ é *fortemente κ-homogênea* se, para todos $X \subseteq A$ com $|X| < \kappa$ e $f : X \to A$ tal que $(\mathfrak{A}, (x)_{x\in X}) \equiv (\mathfrak{A}, (f(x))_{x\in X})$, f estende-se a um automorfismo de $\mathfrak{A}$. Desse modo, quaisquer dois elementos $a, b \in A^m$ que satisfazem o mesmo tipo sobre X são conjugados por um automorfismo sobre X, considerando-se $(\mathfrak{A}, (x)_{x\in X}, a) \equiv (\mathfrak{A}, (x)_{x\in X}, b)$.

Teorema 1.4.4. Para $\kappa > |\mathrm{L}|$, κ-saturação equivale a κ-homogeneidade e κ-universalidade simultâneas.

Demonstração: Como é usual, provaremos que κ-saturação implica κ-homogeneidade e κ^+-universalidade. Já que κ^+-universalidade implica trivialmente κ-universalidade, deveremos também provar que κ-homogeneidade e κ-universalidade simultâneas implicam κ-saturação. Neste momento, faremos uso da hipótese $\kappa > |\mathrm{L}|$.

Suponha $\mathfrak{A}$ κ-saturada: o Lema 1.4.3 implica que $\mathfrak{A}$ é κ-homogênea. Suponha então $\mathfrak{B} \equiv \mathfrak{A}$ com $|B| < \kappa^+$, ou seja, $|B| \leqslant \kappa$. Seja $(b_\xi)_{\xi<|B|}$ uma enumeração sem repetições dos elementos de B. Definiremos $a_\xi \in A$, $\xi < |B|$, indutivamente: assuma que, para $\xi < |B|$, $(a_\zeta)_{\zeta<\xi}$ esteja definida de modo que $(\mathfrak{A}, (a_\zeta)_{\zeta<\xi}) \equiv (\mathfrak{B}, (b_\zeta)_{\zeta<\xi})$. (O caso $\xi = 0$ é nossa condição inicial.) O conjunto $\{b_\zeta \mid \zeta < \xi\}$ tem cardinalidade $|\xi| < |B| \leqslant \kappa$. Pelo lema anterior, existe $a_\xi \in A$ tal que $(\mathfrak{A}, (a_\zeta)_{\zeta\leqslant\xi}) \equiv (\mathfrak{B}, (b_\zeta)_{\zeta\leqslant\xi})$. Aqui podemos observar que, por sentenças terem apenas um número finito de constantes, as equivalências da indução implicam $(\mathfrak{A}, (a_\xi)_{\xi<|B|}) \equiv (\mathfrak{B}, (b_\xi)_{\xi<|B|})$. Como $(b_\xi)_{\xi<|B|}$ enumera B, a função que leva b_ξ a a_ξ é uma imersão elementar de $\mathfrak{B}$ em $\mathfrak{A}$. Concluímos que $\mathfrak{A}$ é κ^+-universal.

Suponha agora que $\mathfrak{A}$ é κ-homogênea e κ-universal. Sejam $X \subseteq A$ com $|X| < \kappa$ e $p \in S_m(X)$. Substitua as variáveis livres de p por uma seqüência c de novas constantes, obtendo uma teoria $T = p(c) \cup Th(\mathfrak{A}, (x)_{x\in X})$ em uma linguagem de cardinal $|\mathrm{L}(X)| + m < \kappa$. (T é consistente por definição.) Há então um modelo $(\mathfrak{B}, (b_x)_{x\in X}, b)$ de T, com $|B| < \kappa$ pelo Teorema de Löwenheim–Skolem, em que b interpreta as constantes c. Temos $\mathfrak{B} \equiv \mathfrak{A}$, havendo por κ-universalidade uma imersão elementar de $\mathfrak{B}$ em $\mathfrak{A}$ que assumiremos ser uma inclusão, ou seja, $\mathfrak{B} \prec \mathfrak{A}$. Então

$$(\mathfrak{A}, (x)_{x\in X}) \equiv (\mathfrak{B}, (b_x)_{x\in X}) \equiv (\mathfrak{A}, (b_x)_{x\in X})$$

e, por κ-homogeneidade, existe $a \in A^m$ tal que

$$(\mathfrak{A}, (x)_{x\in X}, a) \equiv (\mathfrak{A}, (b_x)_{x\in X}, b) \equiv (\mathfrak{B}, (b_x)_{x\in X}, b) .$$

Assim, a realiza p em $(\mathfrak{A}, (x)_{x\in X})$ porque $(\mathfrak{A}, (b_x)_{x\in X}) \models p(b)$. Concluímos que $\mathfrak{A}$ é κ-saturada. QED

Teorema 1.4.5. κ-homogeneidade forte implica κ-homogeneidade. Se $\mathfrak{A}$ é $|A|$-homogênea então $\mathfrak{A}$ é fortemente $|A|$-homogênea.

Demonstração: A primeira afirmação é simples: sendo $\mathfrak{A}, X, Y, a$ como na definição de κ-homogeneidade e nomeando $f : X \to Y$ a bijeção, tome b a imagem de a pelo automorfismo que estende f.

Para a segunda, podemos proceder por indução finita se $|A| < \omega$: obtemos o automorfismo quando aplicamos a definição ao caso $|X| = |A| - 1$ e $a \notin X$. Suponha então $\mathfrak{A}$ infinita.

Assuma que $\mathfrak{A}$ é $|A|$-homogênea e suponha $X \subseteq A$ com $|X| < |A|$ e $f : X \to A$ tal que $(\mathfrak{A}, (x)_{x\in X}) \equiv (\mathfrak{A}, (f(x))_{x\in X})$. Vemos que f é uma injeção; como na definição de homogeneidade, convém chamar $Y = f[X]$.

Indexe sem repetições $A - X = \{x_\xi\}_{\xi<|A|}$ e $A - Y = \{y_\xi\}_{\xi<|A|}$. Definiremos indutivamente seqüências $(c_\xi)_{\xi<|A|}$, $(d_\xi)_{\xi<|A|}$ sem repetições. Assuma $\xi < |A|$ e $(c_\zeta, d_\zeta)_{\zeta<\xi}$ já definida de modo que

$$(\mathfrak{A}, (x)_{x\in X}, (c_\zeta)_{\zeta<\xi}) \equiv (\mathfrak{A}, (f(x))_{x\in X}, (d_\zeta)_{\zeta<\xi}) .$$

(O caso $\xi = 0$ é dado por hipótese.) Lembramos agora que ξ escreve-se de modo único como $\xi = \lambda + n$, em que λ é um ordinal limite (ou 0) e $n < \omega$.

Se n é par, tome $c_\xi = x_{\lambda+n/2}$. Já que $\mathfrak{A}$ é homogênea e $|X \cup \{c_\zeta\}_{\zeta<\xi} \cup \{c_\xi\}| \leqslant |X| + |\xi| + 1 < |A|$, existe $d_\xi \in A$ tal que

$$(\mathfrak{A}, (x)_{x\in X}, (c_\zeta)_{\zeta\leqslant\xi}) \equiv (\mathfrak{A}, (f(x))_{x\in X}, (d_\zeta)_{\zeta\leqslant\xi}) .$$

Essa equivalência elementar mostra que $d_\xi \in (A - Y) - \{d_\zeta \mid \zeta < \xi\}$.

Se n é ímpar, proceda analogamente, mas tomando $d_\xi = y_{\lambda+(n-1)/2}$ e obtendo $c_\xi \in (A - X) - \{c_\zeta \mid \zeta < \xi\}$.

Completada a indução, defina $\sigma(x) = f(x)$ para $x \in X$ e $\sigma(c_\xi) = d_\xi$ para $\xi < |A|$. Por construção, o domínio de σ é todo A: os casos pares acima exaurem $A - X$, notadamente $x_{\lambda+k} = c_{\lambda+2k}$. Também a imagem de σ é todo A, porque os casos ímpares exaurem $A - Y$, notadamente $y_{\lambda+k} = d_{\lambda+2k+1}$. Obtemos $(\mathfrak{A}, (x)_{x\in X}, (c_\xi)_{\xi<|A|}) \equiv (\mathfrak{A}, (f(x))_{x\in X}, (d_\xi)_{\xi<|A|})$, ou seja, $(\mathfrak{A}, (a)_{a\in A}) \equiv (\mathfrak{A}, (\sigma(a))_{a\in A})$, de modo que σ é um automorfismo de $\mathfrak{A}$ que estende f. QED

Existe uma curiosa equivalência entre conceitos geométricos e algébricos:

Proposição 1.4.6. Suponha $\mathfrak{A}$ κ-saturada e fortemente κ-homogênea e $X \subseteq A$ com $|X| < \kappa$. Um definível é X-definível se e somente se é invariante sob todos os automorfismos sobre X.

Demonstração: Seja D um subconjunto definível de A^m. Suponha que $D = \phi(\mathfrak{A}, a)$, com ϕ de L e $a \in X^n$, e que ξ seja um automorfismo sobre X. Como $\xi(a) = a$, temos $\xi[D] = \phi(\mathfrak{A}, \xi(a)) = \phi(\mathfrak{A}, a) = D$.

Suponha agora que $D = \phi(\mathfrak{A}, a)$ com $a \in A^n$, ou seja, D é um definível arbitrário, e que D seja fixado por todos os automorfismos sobre X. Se D é vazio, é claro que é X-definível: assumiremos então $D \neq \emptyset$. Sendo v uma seqüência de m variáveis, consideraremos $\Phi(v)$ o conjunto contendo $\neg\phi(v, a)$ e as fórmulas de L(X) satisfeitas por todas as m-uplas de D. Note que $|Xa| < \kappa$.

Primeiramente, mostremos que Φ não é satisfazível em $\mathfrak{A}$. Suponha $\alpha \in A^m$ tal que $\mathfrak{A} \models \Phi(\alpha)$: então $\alpha \notin D$, mas α satisfaz todas as fórmulas de L(X) satisfeitas pelas m-uplas de D. Desse modo, sendo $d = (d_1, \ldots, d_m) \in D$ arbitrária, temos $(\mathfrak{A}, (x)_{x\in X}, d) \equiv (\mathfrak{A}, (x)_{x\in X}, \alpha)$. Note que também $|Xd| < \kappa$. Definindo $f : Xd \to X\alpha$ com $f|_X$ a identidade e $f(d_i) = \alpha_i$ — tal f está bem definida pela equivalência elementar —, f estende-se a um automorfismo f^* de $\mathfrak{A}$ por sua κ-homogeneidade forte. Ora, f^* é um automorfismo sobre X, mas não fixa D pois $f^*(d) = \alpha \notin D$, contrariando nossa hipótese.

Pela κ-saturação de $\mathfrak{A}$, um subconjunto finito Φ_0 de Φ também não é realizado em $\mathfrak{A}$. É claro que $\neg\phi(v, a) \in \Phi_0$, sendo $D \neq \emptyset$. Podemos supor que há outras fórmulas em Φ_0, acrescentando qualquer uma de Φ.

Tome $\psi(v)$ a fórmula de L(X) conjunção de todas as fórmulas de Φ_0 exceto $\neg\phi(v, a]$. Por definição, se $d \in D$ então $\mathfrak{A} \models \psi(d)$; reciprocamente, se $\alpha \in A^m$ realiza ψ então $\alpha \in D$, pois caso contrário $\mathfrak{A} \models \Phi_0(\alpha)$. Concluímos que $D = \psi(\mathfrak{A})$ e que D é X-definível. QED

Corolário 1.4.7. Nessas condições, um subconjunto finito de A^m é X-definível se e somente se é invariante sob todos os automorfismos sobre X. Desse modo, uma m-upla $a \in A^m$ é X-definível se e somente se todo automorfismo sobre X fixa a.

Na proposição, a condição de já ser definível não pode ser removida, como este exemplo conclui com $X = \emptyset$:

Exemplo 1.4.8. $\mathbb{N}$ com sua ordem usual tem uma extensão elementar ω_1-saturada e fortemente ω_1-homogênea $\mathfrak{C}$ (veremos isso no Teorema 1.4.11), que podemos assumir *própria*, tomando antes uma extensão elementar de $\mathbb{N}$ que o seja. Sabemos que todos os novos elementos de C são finais, ou seja, são precedidos por todos os naturais.

Assim, $\mathbb{N}$ é invariante sob todos os automorfismos (de ordem) de $\mathfrak{C}$. De fato, suponha que um tal automorfismo ξ leve $n \in \mathbb{N}$ a $C - \mathbb{N}$. Podemos supor que n é mínimo com essa propriedade. Como $\xi(0) = 0$ (0 é o elemento mínimo de $\mathfrak{C}$), temos $n \neq 0$. Então $\xi(n-1) \in \mathbb{N}$ e existem naturais maiores que $\xi(n-1)$, portanto entre $\xi(n-1)$ e $\xi(n)$, de modo que ξ não é um automorfismo.

Porém, $\mathbb{N}$ não é $\emptyset$-definível em $\mathfrak{C}$ por ser uma subestrutura elementar própria. De fato, se ϕ é uma fórmula sem parâmetros tal que $\mathbb{N} = \phi(\mathfrak{C})$, então para todo $n \in \mathbb{N}$ temos $\mathfrak{C} \models \phi(n)$, donde $\mathbb{N} \models \phi(n)$ e conclui-se que $\mathbb{N} \models \forall v\, \phi(v)$, mas essa sentença não vale em $\mathfrak{C}$, contradição.

Há muitas outras propriedades de estruturas com hipótese de (κ-)saturação, homogeneidade ou universalidade, que não apresentaremos por não serem centrais ao nosso desenvolvimento, embora importantes por si mesmas. Porém, o leitor interessado pode consultar o Capítulo 5 de [Chang, Keisler], o Capítulo 10 de [Hodges] ou o Capítulo 9 de [Poizat 1].

Essas que vimos, porém, sugerem que seja interessante trabalhar em estruturas saturadas, especificamente pela homogeneidade forte. Mencionaremos no Teorema 2.3.14 que teorias importantes, chamadas estáveis, têm modelos saturados. Contudo, a existência de modelos saturados de teorias arbitrárias condiciona-se à Hipótese Generalizada do Contínuo ou à existência de cardinais inaccessíveis muito grandes — esta, aliás, é a condição em que [Shelah] trabalha (p. 7–8) —, como indicam a Proposição 5.1.5 e o Exercício 5.1.4 de [Chang, Keisler] e os Exercícios 6, 7 e 8 da Seção 10.4 de [Hodges]. Tal dificuldade é observada em [MTAG], que assume então a construção de uma classe própria com as características desejadas.

Optamos por seguir a sugestão de [Pillay] e introduzir as estruturas κ-grandes de [Hodges]. De modo a não depender extraordinariamente deste texto, delinearemos as demonstrações pertinentes. Adaptamos resultados e exemplos de suas Seções 10.1 e 10.2, mas alteramos alguma notação e conteúdo. O leitor também pode explorar o conceito análogo de κ-resplendência exposto em [Poizat 1], de onde derivamos alguns raciocínios.

$\mathfrak{A}$ é κ-*grande* se, para todo $X \subseteq A$ com $|X| < \kappa$, vale esta propriedade: "Adicione a $L(X)$ um novo predicado. Se $(\mathfrak{B}, (b_x)_{x \in X}) \equiv (\mathfrak{A}, (x)_{x \in X})$ e S é uma relação em B, então existe uma relação R em A tal que $(\mathfrak{B}, (b_x)_{x \in X}, S) \equiv (\mathfrak{A}, (x)_{x \in X}, R)$."

Vemos que toda estrutura finita é κ-grande, porque $\equiv$ e $\cong$ são noções idênticas para estruturas finitas.

O Exemplo 4 da Seção 10.1 de [Hodges] informa que um corpo algebricamente fechado K de grau de transcendência infinito sobre seu corpo primo é $|K|$-grande e menciona que André Weil, em seu *Foundations of Algebraic Geometry* (AMS, 1946), sugeriu que se utilizassem os corpos algebricamente fechados de grau de transcendência infinito como *domínios universais*. O Teorema 9.17 de [Poizat 1] indica que qualquer estrutura saturada, em geral, tem tamanha grandeza. Contentamo-nos em demonstrar uma recíproca:

Teorema 1.4.9. κ-grandeza implica κ-saturação e κ-homogeneidade forte.

Demonstração: Admita que $\mathfrak{A}$ é uma estrutura κ-grande. Para mostrar que é κ-saturada, suponha $X \subseteq A$ com $|X| < \kappa$ e $p \in S_m(X)$. Sejam $\mathfrak{B}$ uma extensão elementar de $\mathfrak{A}$ e $b \in B^m$ de modo que $p = t(b/X)$. Temos $(\mathfrak{B}, (x)_{x \in X}) \equiv (\mathfrak{A}, (x)_{x \in X})$, existindo $R \subseteq A^m$ tal que $(\mathfrak{B}, (x)_{x \in X}, \{b\}) \equiv (\mathfrak{A}, (x)_{x \in X}, R)$. Pela equivalência elementar, vemos que R é unitário, contendo uma m-upla a. Concluímos que as fórmulas que são realizadas por b em $(\mathfrak{B}, (x)_{x \in X})$ são realizadas por a em $(\mathfrak{A}, (x)_{x \in X})$, considerando-as como sentenças da linguagem estendida. Assim, $(\mathfrak{A}, (x)_{x \in X}) \models p(a)$.

Para mostrar que $\mathfrak{A}$ é fortemente κ-homogênea, suponha agora $X \subseteq A$ com $|X| < \kappa$ e $f : X \to A$ tal que $(\mathfrak{A}, (x)_{x \in X}) \equiv (\mathfrak{A}, (f(x))_{x \in X})$. Tome um novo predicado binário P e considere, na linguagem apropriada, o conjunto T das sentenças (i) em $Th(\mathfrak{A}, (x)_{x \in X}, (f(x))_{x \in X})$, (ii) $\forall u \exists^{=1} v\, P(u, v)$, $\forall v \exists^{=1} u\, P(u, v)$, (iii) $P(x, f(x))$ para cada $x \in X$, (iv) para cada fórmula atômica ϕ de L, com n variáveis livres,

$$\forall u_1 \ldots \forall u_n \forall v_1 \ldots \forall v_n \Big(\bigwedge_{i=1}^{n} P(u_i, v_i) \to (\phi(u_1, \ldots, u_n) \leftrightarrow \phi(v_1, \ldots, v_n)) \Big) .$$

Primeiramente, mostremos que T é finitamente satisfazível. Dado X_0 um subconjunto finito de X, seja $\overline{x}$ uma $|X_0|$-upla contendo cada elemento de X_0 sem repetição. Temos $(\mathfrak{A}, \overline{x}) \equiv (\mathfrak{A}, f(\overline{x}))$, de modo que $\overline{x}$ e $f(\overline{x})$ realizam as mesmas fórmulas de L e então têm o mesmo $|X_0|$-tipo sobre $\emptyset$. Pela Proposição 1.3.9, existem $\mathfrak{B}$ uma extensão elementar de $\mathfrak{A}$ e ξ um automorfismo de $\mathfrak{B}$ com $\xi(\overline{x}) = f(\overline{x})$. Seja S o gráfico de ξ, para interpretar P. Temos

$(\mathfrak{B},(x)_{x\in X},(f(x))_{x\in X})\equiv(\mathfrak{A},(x)_{x\in X},(f(x))_{x\in X})$ e $(\mathfrak{B},S)$ satisfaz as sentenças (ii) e (iv), porque ξ é um automorfismo, e também $P(x,f(x))$ para cada $x\in X_0$.

Então T é consistente e tem um modelo que escreveremos com repetição das letras: $(\mathfrak{B},(b_x)_{x\in X},(c_x)_{x\in X},S)$, em que b_x, c_x interpretam as constantes de $x, f(x)$ respectivamente. Pela definição de T, temos $(\mathfrak{B},(b_x)_{x\in X},(c_x)_{x\in X})\equiv(\mathfrak{A},(x)_{x\in X},(f(x))_{x\in X})$. Pela equivalência elementar, os elementos de $X\cap f[X]$ correspondem exatamente aos $b_x=c_x$, $x\in X$, porque $\mathfrak{B}\models b_x=c_y \Leftrightarrow \mathfrak{A}\models x=f(y)$. Então podemos considerar $(\mathfrak{B},(b)_{b\in\{b_x,c_x\mid x\in X\}})\equiv(\mathfrak{A},(x)_{x\in X\cup f[X]})$. Temos $|X\cup f[X]|\leqslant|X|+|X|<\kappa$. Como $\mathfrak{A}$ é κ-grande, existe $R\subseteq A^2$ tal que $(\mathfrak{B},(b)_{b\in\{b_x,c_x\mid x\in X\}},S)\equiv(\mathfrak{A},(x)_{x\in X\cup f[X]},R)$. Pelas sentenças (ii), R é o gráfico de uma bijeção $\xi : A\to A$; pelas (iii), ξ estende f; pelas (iv), ξ é automorfismo de $\mathfrak{A}$. QED

Precisamos agora do resultado conhecido como "Lema da consistência (conjunta) de Robinson":

Teorema 1.4.10 (Robinson). Suponha $\mathrm{L}_1,\mathrm{L}_2$ duas linguagens cujos símbolos em comum formem a linguagem L_0, mas reunidas formem a linguagem L. Sejam T_1, T_2 teorias de $\mathrm{L}_1,\mathrm{L}_2$ respectivamente. Se $T_1\cap T_2$ é uma teoria completa de L_0, então $T_1\cup T_2$ é uma teoria de L e diz-se que T_1 é *consistente com* T_2.

Referências: O Teorema 2.2.23 de [Chang, Keisler] ou o Exercício 6.6.1 de [Hodges], derivado de seu teorema de mesmo número. Ambos os textos têm outras demonstrações.

Teorema 1.4.11. Se $\kappa>|\mathrm{L}|$ e κ é regular, então toda L-estrutura $\mathfrak{A}$ tem uma extensão elementar κ-grande $\mathfrak{B}$ tal que $|B|\leqslant|A|^{<\kappa}$.

Demonstração: Se α,β são cardinais, $\alpha^{<\beta}=\sup\{\alpha^\rho\mid\rho \text{ cardinal} <\beta\}$: por exemplo, $2^{<\omega}=\omega$. Também faremos uso do produto $\xi\bullet\zeta$ de dois ordinais ξ e ζ, que corresponde a cópias de ξ ordenadas por ζ. A discussão acima nos permite assumir que $\mathfrak{A}$ é infinita.

Tome $\mu=|A|^{<\kappa}$, de modo que $\mu=\mu^{<\kappa}\geqslant\kappa>|\mathrm{L}|$. Pelo uso constante, chamaremos os ordinais $<\mu\bullet(\mu\bullet\kappa)$ de *testemunhas.*

Podemos indexar com repetições $(X_\xi,T_\xi)_{0<\xi<\mu\bullet\kappa}$ os pares (X_ξ,T_ξ) em que X_ξ é um conjunto de menos de κ testemunhas e T_ξ é uma teoria completa na linguagem obtida de $\mathrm{L}(X_\xi)$ adicionando-se um predicado P_ξ, de modo que cada par aparece com freqüência cofinal na lista. Para verificar a indexação, note que $\mu\bullet\kappa$ são κ blocos de comprimento μ. Suponha que $\nu<\kappa$ é um cardinal: o número de conjuntos de ν testemunhas é $\mu^\nu=\mu$ e o número de tais teorias completas é $\leqslant 2^{|\mathrm{L}|+\nu+1}\omega\leqslant\mu^{<\kappa}=\mu$.

Construiremos uma cadeia elementar de estruturas $\mathfrak{A}_\xi$, $0 < \xi < \mu \bullet \kappa$, em que $A_\xi = \mu \bullet \xi$. Indicaremos $(\mathfrak{A}_\xi, \ldots)$ uma estrutura que expande $\mathfrak{A}_\xi$. A construção será tal que, se $\xi \geqslant \zeta$, a linguagem de $(\mathfrak{A}_\xi, \ldots)$ é uma expansão da de $(\mathfrak{A}_\zeta, \ldots)$, e a cadeia será elementar para cada linguagem, a partir da primeira estrutura apropriada.

Pelo Teorema de Löwenheim–Skolem, $\mathfrak{A}$ tem uma extensão elementar $\mathfrak{A}_1$ de cardinal μ; identificamos A_1 e o ordinal $\mu \bullet 1 = \mu$. Faremos ainda outras identificações análogas, via bijeções que transformamos em isomorfismos.

Se $\lambda < \mu$ é um ordinal limite, tome $(\mathfrak{A}_\lambda, \ldots) = \bigcup_{0<\xi<\lambda} (\mathfrak{A}_\xi, \ldots)$.

Assuma que $(\mathfrak{A}_\xi, \ldots)$ foi definida com domínio $\mu \bullet \xi$. Considere o par (X_ξ, T_ξ). Se alguma testemunha $\geqslant \mu \bullet \xi$ pertence a X_ξ ou se a teoria T_ξ é inconsistente com o diagrama elementar de $(\mathfrak{A}_\xi, \ldots)$, tome $(\mathfrak{A}_{\xi+1}, \ldots)$ uma extensão elementar arbitrária de $(\mathfrak{A}_\xi, \ldots)$ com domínio $\mu \bullet (\xi + 1)$. Isso é possível com o Adendo ao Teorema de Löwenheim–Skolem.

Suponha agora que cada testemunha em X_ξ é um elemento de A_ξ e que a teoria T_ξ é consistente com o diagrama elementar de $(\mathfrak{A}_\xi, \ldots)$. (Neste ponto ocorrerá expansão da linguagem.) Alguma extensão elementar $(\mathfrak{D}, \ldots)$ de $(\mathfrak{A}_\xi, \ldots)$, com também alguma interpretação para $(x)_{x \in X_\xi}$ e P_ξ, é modelo de T_ξ. Por Löwenheim–Skolem, podemos supor que $|D| = \mu$ e que os elementos de D são os ordinais $< \mu \bullet (\xi + 1)$. Desse modo, tome $(\mathfrak{A}_{\xi+1}, \ldots) = (\mathfrak{D}, \ldots)$ com suas novas interpretações.

Tome agora $(\mathfrak{B}, \ldots) = \bigcup_{0<\xi<\mu\bullet\kappa} (\mathfrak{A}_\xi, \ldots)$. Vemos que $\mathfrak{B}$ é uma extensão elementar de $\mathfrak{A}$ e $B = \mu \bullet (\mu \bullet \kappa)$ tem cardinalidade μ. Reduzida à linguagem apropriada, $(\mathfrak{B}, \ldots)$ também é extensão elementar de cada $(\mathfrak{A}_\xi, \ldots)$.

Mostremos que $\mathfrak{B}$ é κ-grande. Suponha $X \subseteq B$ com $|X| < \kappa$ e $\mathfrak{D}$ tal que $(\mathfrak{D}, (d_x)_{x \in X}) \equiv (\mathfrak{B}, (x)_{x \in X})$; seja S uma relação em D. Já que κ é regular, $\mu \bullet \kappa$ é um ordinal de cofinalidade κ e existe $\zeta < \mu \bullet \kappa$ tal que todas as testemunhas em X são menores que $\mu \bullet \zeta$, donde $X \subseteq A_\zeta$ e $(\mathfrak{D}, (d_x)_{x \in X}) \equiv (\mathfrak{A}_\zeta, (x)_{x \in X})$. Pela forma da indexação, existe $\xi \geqslant \zeta$ tal que $X_\xi = X$ e $T_\xi = Th(\mathfrak{D}, (d_x)_{x \in X}, S)$. Ao mostrar que T_ξ é consistente com o diagrama elementar de $(\mathfrak{A}_\xi, \ldots)$, obtemos $(\mathfrak{A}_{\xi+1}, \ldots)$ modelo de T_ξ, e então $(\mathfrak{B}, (x)_{x \in X})$ expande-se a um modelo de T_ξ como desejado.

Como $\mathfrak{A}_\zeta \prec \mathfrak{A}_\xi$ e $X \subseteq A_\zeta$, temos $(\mathfrak{A}_\zeta, (x)_{x \in X}) \equiv (\mathfrak{A}_\xi, (x)_{x \in X})$, donde $(\mathfrak{D}, (d_x)_{x \in X}) \equiv (\mathfrak{A}_\xi, (x)_{x \in X})$. Então

$$T_\xi \cap Th(\mathfrak{A}_\xi, \ldots, (a)_{a \in A_\xi}) = Th(\mathfrak{A}_\xi, (x)_{x \in X}) \; ,$$

sendo a linguagem apropriada a comum dentre as duas originais. Basta então aplicar o Teorema de Robinson. QED

Assim, tomemos κ regular e maior que $|\mathrm{L}|$ e a cardinalidade das estruturas e conjuntos de parâmetros trabalhados, um cardinal *sucessor* por exemplo. Assuma agora que T seja uma teoria *completa* de L *com modelos infinitos*. Pelo Teorema de Löwenheim–Skolem, T tem um modelo de cardinal $|\mathrm{L}|$. Por este teorema, tal modelo estende-se a outro κ-grande $\mathfrak{C}$ de cardinal no máximo $|\mathrm{L}|^{<\kappa}$. Então $\mathfrak{C}$ é κ-grande, κ-saturado, fortemente κ-homogêneo e κ-universal. Por T ser completa, $\mathfrak{C}$ estende elementarmente todos os modelos infinitos de T de cardinal $< \kappa$. $\mathfrak{C}$ é chamado o *modelo monstro* de T, dentro do qual se trabalha como em um domínio universal.

Freqüentemente, a literatura escreve apenas $\vDash \phi(c)$ ou $\models \phi(c)$ para $\phi(v_1, \ldots, v_n)$ fórmula de L e $c \in C^n$, abreviando as afirmações (equivalentes porque T é completa) $\mathfrak{C} \models \phi(c)$ e $T \vDash \phi(c)$ considerada como sentença de $\mathrm{L}(C)$.

O modelo monstro é indicado $\mathfrak{C}$ em [MTAG] e [Shelah], $\mathbf{C}$ em [Pillay], e de muitas outras formas. Em algumas ocasiões, é apenas preciso uma extensão elementar de uma dada estrutura $\mathfrak{A}$ como no próprio Teorema 1.4.11, preferencialmente com $\kappa > |A|$. [Marker] indica tal modelo monstro como $M \prec \mathbb{M}$ ou $G \prec \mathbb{G}$.

Usaremos normalmente as letras $\mathfrak{C}$ e C como estrutura e domínio quaisquer.

Quando trabalharmos em um modelo monstro, introduziremos sua "versão" e a notação necessária. Em geral, escreveremos o cardinal de sua grandeza, embora freqüentemente bastem condições mais fracas de saturação e/ou homogeneidade forte. Adiantamos que, em diversas ocasiões, adotaremos o mesmo padrão: dada $\mathfrak{A}$, tomamos $\mathfrak{B}$ uma extensão elementar ω-saturada e, de $\mathfrak{B}$, uma extensão elementar $|B|^+$-grande $\mathfrak{C}$.

2
Introdução à Estabilidade

Introduziremos, neste capítulo, conceitos e ferramentas fundamentais na Teoria dos Modelos. O posto de Morley de um conjunto definível, como apresentaremos na primeira seção, é uma noção de dimensão simultaneamente intrínseca à Estabilidade e relacionada com noções particulares da Matemática. O espaço de tipos, por outro lado, contém amplas informações sobre seus modelos e os resultados de Estabilidade que apresentaremos conectam ambos os conceitos de modo preciso. Uma terceira fonte/aplicação de noções e resultados em Estabilidade advém de estudos sobre a classificação de teorias e dos modelos de uma teoria, conduzidos principalmente por Shelah e que não conheceremos aqui.

Trabalharemos com uma linguagem fixada L, porém arbitrária; outras hipóteses variam de seção para seção e são explicitadas em suas introduções. Consideraremos tipos como ultrafiltros de definíveis, depois como conjuntos de fórmulas. Como usual, escreveremos apenas RMI, dM e afins quando o contexto permitir. Por todo o capítulo, letras gregas minúsculas são ordinais, ou fórmulas quando assim apresentadas.

Originalmente, redigimos este capítulo seguindo o tratamento de [Ziegler], embora aqui suas "classes" sejam conjuntos, e adaptando material de [Pillay] e [Hodges]. Note que [Pillay], [Shelah] e [Ziegler] trabalham em um modelo monstro, onde muitas de nossas colocações (restritivas) não são aparentes. Outras referências gerais para Estabilidade são J. T. Baldwin, *Fundamentals of Stability Theory*, Springer-Verlag, 1988, e D. Lascar, *Stability in Model Theory*, Longman Scientific and Technical, 1987 (tradução de J. E. Wallington do original em francês *Stabilité en Théorie des Modèles*).

2.1. Posto de Morley para definíveis

Começamos por definir um "posto de Morley interno" $\mathrm{RMI}_{\mathfrak{A}}$. A Seção 5.6 de [Hodges] chama-o de "posto de Cantor–Bendixson" e indica $\mathrm{RCB}_{\mathfrak{A}}$. Na Seção 6.2 de [Marker], é indicado $\mathrm{RM}^{\mathfrak{A}}$; reservaremos, porém, a notação $\mathrm{RM}_{\mathfrak{A}}$ para o posto geral.

Expandiremos formalmente a definição usual e deduziremos suas propriedades básicas. Note que $\mathrm{RMI}_{\mathfrak{A}}$ e $\mathrm{dMI}_{\mathfrak{A}}$ serão definidos para *todos* os definíveis; por exemplo, na definição de $\mathrm{rmi}_{\mathfrak{A}}(D) \geqslant \xi + 1$ abaixo, os definíveis D_i têm *quaisquer* parâmetros em A, sejam os mesmos de D ou não. Esse procedimento será essencial para a comparação de tipos sobre conjuntos diferentes (privilegiará os tipos globais) e para maleabilidade dos enunciados: por exemplo, a Proposição 2.1.14.

Fixe uma L-estrutura $\mathfrak{A}$. Começamos por supor $D, E, F \in \mathrm{Def}^m_A$, embora façamos outras hipóteses adiante.

Uma motivação simples é dada em [Marker]. Suponha V um espaço vetorial de dimensão n sobre um corpo infinito K e $f : V \to K$ um funcional linear não-nulo. Para cada $a \in K$, $V_a = \{v \in V \mid f(v) = a\}$ é um subconjunto de V de dimensão afim $n-1$, ou seja, translação do núcleo V_0 de dimensão $n-1$, e evidentemente $\{V_a\}_{a \in K}$ é uma família infinita de conjuntos dois a dois disjuntos.

Para esta definição e uso relacionado posterior, note que $D_i \in \mathrm{Def}^m_{\mathfrak{A},A}$.

Definição 2.1.1. Por recursão transfinita, definimos a relação:

$\mathrm{rmi}_{\mathfrak{A}}(D) \geqslant 0 \Leftrightarrow D \neq \emptyset$;

$\mathrm{rmi}_{\mathfrak{A}}(D) \geqslant \lambda$ limite $\Leftrightarrow \mathrm{rmi}_{\mathfrak{A}}(D) \geqslant \xi$ para todo $\xi < \lambda$;

$\mathrm{rmi}_{\mathfrak{A}}(D) \geqslant \xi + 1 \Leftrightarrow$ existe uma família infinita de definíveis dois a dois disjuntos $D_i \subseteq D$, $i \in I$, tais que $\mathrm{rmi}_{\mathfrak{A}}(D_i) \geqslant \xi$ para todo $i \in I$.

Podemos permutar, sempre, I com $\mathbb{N}$.

Embora essa relação entre D e ξ seja indicada por $\mathrm{rmi}(\cdot) \geqslant$, o símbolo $\geqslant$ sugere uma relação de transitividade que verificamos na

Proposição 2.1.2. Se $\mathrm{rmi}(D) \geqslant \xi$ e $\xi \geqslant \zeta$ então $\mathrm{rmi}(D) \geqslant \zeta$.

Demonstração: Procedemos por indução em ξ, para qualquer definível. Suponha $\zeta < \xi$ e assuma que $\mathrm{rmi}(D) \geqslant \xi$.

Se $\xi = 0$, não existe tal ζ e o resultado é trivialmente verdadeiro. Se ξ é um ordinal limite, por definição $\mathrm{rmi}(D) \geqslant \zeta$.

Seja então $\xi = \delta + 1$, de modo que $\zeta \leqslant \delta$ e δ tem a propriedade enunciada.

Suponha que ζ é um ordinal limite e $\eta < \zeta$. Como $\eta < \delta$, por hipótese vem $\mathrm{rmi}(D) \geqslant \eta$. Desse modo, $\mathrm{rmi}(D) \geqslant \zeta$ por definição.

Suponha finalmente que $\zeta = \eta + 1$. Existem definíveis dois a dois disjuntos $D_i \subseteq D$, $i \in I$ infinito, tais que $\mathrm{rmi}(D_i) \geqslant \delta$ para todo $i \in I$. Por hipótese, já que $\eta < \delta$, vale $\mathrm{rmi}(D_i) \geqslant \eta$ para todo $i \in I$. Por definição, $\mathrm{rmi}(D) \geqslant \eta + 1 = \zeta$.

QED

Definição 2.1.3. Tome $\mathrm{RMI}_{\mathfrak{A}}(D) = \sup\{\xi \mid \mathrm{rmi}_{\mathfrak{A}}(D) \geqslant \xi\}$, chamado *posto de Morley interno* de D em $\mathfrak{A}$. (Em inglês, RM abrevia *Morley rank*, com a inversão tradicional devida à escola parisiense; escreve-se também MR.)

Conforme nossa convenção, temos $\mathrm{RMI}_{\mathfrak{A}}(\emptyset) = -1$ e $\mathrm{RMI}_{\mathfrak{A}}(D) = \infty$ se $\mathrm{rmi}_{\mathfrak{A}}(D) \geqslant \xi$ para todo ordinal ξ, casos em que se diz que D *não tem posto interno*.

Note que $\mathrm{RMI}(D) \geqslant \xi \Leftrightarrow \mathrm{rmi}(D) \geqslant \xi$. Essa equivalência se mostrará muito útil, em especial porque $\mathrm{RMI}(D) \geqslant \xi + 1 \Leftrightarrow$ existem definíveis dois a dois disjuntos $D_n \subseteq D$, $n \in \mathbb{N}$, tais que $\mathrm{RMI}(D_n) \geqslant \xi$.

Vemos que: $\mathrm{RMI}(D) = 0 \Leftrightarrow D$ é finito não-vazio; $\mathrm{RMI}(D) = 1 \Leftrightarrow D$ é infinito e não contém uma família infinita de definíveis dois a dois disjuntos.

Faremos repetido uso desta proposição e de seu corolário:

Proposição 2.1.4. $\mathrm{RMI}(D \cup E) = \max\{\mathrm{RMI}(D), \mathrm{RMI}(E)\}$.

Demonstração: Mostraremos por indução que $\mathrm{rmi}(D \cup E) \geqslant \xi$ se e somente se $\mathrm{rmi}(D) \geqslant \xi$ ou $\mathrm{rmi}(E) \geqslant \xi$, independentemente dos definíveis. Para $\xi = 0$, notamos que $D \cup E \neq \emptyset \Leftrightarrow D$ ou E não é vazio. Usaremos o símbolo $\not\geqslant$ para negar a relação $\mathrm{rmi}(\cdot)\geqslant$.

Suponha que λ é um ordinal limite. Por definição, $\mathrm{rmi}(D \cup E) \geqslant \lambda \Leftrightarrow \mathrm{rmi}(D \cup E) \geqslant \xi$ para todo $\xi < \lambda$; por hipótese, isso ocorre se e somente se $\mathrm{rmi}(D) \geqslant \xi$ ou $\mathrm{rmi}(E) \geqslant \xi$ para cada $\xi < \lambda$. Assim, se $\mathrm{rmi}(D) \geqslant \lambda$ ou $\mathrm{rmi}(E) \geqslant \lambda$, temos $\mathrm{rmi}(D \cup E) \geqslant \lambda$. Assuma então que existem $\xi, \zeta < \lambda$ tais que $\mathrm{rmi}(D) \not\geqslant \xi$ e $\mathrm{rmi}(E) \not\geqslant \zeta$. Para $\eta = \max\{\xi, \zeta\} < \lambda$, temos $\mathrm{rmi}(D) \not\geqslant \eta$ e $\mathrm{rmi}(E) \not\geqslant \eta$ pela proposição anterior e $\mathrm{rmi}(D \cup E) \not\geqslant \eta$, donde $\mathrm{rmi}(D \cup E) \not\geqslant \lambda$.

Tratemos o caso sucessor. Se $\mathrm{rmi}(D) \geqslant \xi + 1$, então existem definíveis dois a dois disjuntos $D_i \subseteq D$, $i \in I$ infinito, tais que $\mathrm{rmi}(D_i) \geqslant \xi$ para todo $i \in I$. Basta observar que $D_i \subseteq D \cup E$ para concluir que $\mathrm{rmi}(D \cup E) \geqslant \xi + 1$. Do mesmo modo, $\mathrm{rmi}(E) \geqslant \xi + 1 \Rightarrow \mathrm{rmi}(D \cup E) \geqslant \xi + 1$.

Assuma que $\mathrm{rmi}(D \cup E) \geqslant \xi + 1$ e sejam $F_i \subseteq D \cup E$, $i \in I$ infinito, definíveis dois a dois disjuntos tais que $\mathrm{rmi}(F_i) \geqslant \xi$ para todo $i \in I$. Por hipótese, para cada $i \in I$ vale: $\mathrm{rmi}(F_i) \geqslant \xi \Leftrightarrow \mathrm{rmi}(D \cap F_i) \geqslant \xi$ ou $\mathrm{rmi}(E \cap F_i) \geqslant \xi$. Assuma ainda que $\mathrm{rmi}(D) \not\geqslant \xi + 1$: devemos mostrar que $\mathrm{rmi}(E) \geqslant \xi + 1$. Por definição, para apenas um número finito de índices $i \in I$ podemos ter $\mathrm{rmi}(D \cap F_i) \geqslant \xi$. Por I ser infinito, para um subconjunto infinito de índices $i \in I$ realmente temos $\mathrm{rmi}(E \cap F_i) \geqslant \xi$, como desejado. QED

Corolário 2.1.5. (i) Por indução, se $D_1, \ldots, D_n \in \mathrm{Def}^m_A$ para $n \geqslant 1$, então $\mathrm{RMI}(D_1 \cup \ldots \cup D_n) = \max_{1 \leqslant i \leqslant n} \mathrm{RMI}(D_i)$.

(ii) Se $D \subseteq E$ então $\mathrm{RMI}(D) \leqslant \mathrm{RMI}(E)$.

Primeiramente, estudemos o "posto" ∞:

Lema 2.1.6. Existe um ordinal ζ tal que qualquer D satisfaz $\mathrm{RMI}(D) \leqslant \zeta$ ou $\mathrm{RMI}(D) = \infty$. (Note que ζ depende de m.)

Demonstração: Já que conjuntos finitos não-vazios são definíveis e têm posto ordinal 0 e Def^m_A é um conjunto, existe o ordinal $\zeta = \sup\{\mathrm{RMI}(D) < \infty \mid D \in \mathrm{Def}^m_A\}$. QED

Lema 2.1.7. Se $\mathrm{RMI}(D) = \infty$, existem dois definíveis disjuntos $D_0, D_1 \subseteq D$ com $\mathrm{RMI}(D_0), \mathrm{RMI}(D_1) = \infty$.

Demonstração: Tome ζ do lema anterior. Então $\mathrm{RMI}(D) \geqslant \zeta + 2$ e existem $D_n \subseteq D$, $n \in \mathbb{N}$, definíveis dois a dois disjuntos com $\mathrm{RMI}(D_n) \geqslant \zeta + 1$. Em particular, $\mathrm{RMI}(D_0), \mathrm{RMI}(D_1) = \infty$. QED

Essa situação é intrigante: como ocorre $\mathrm{RMI}(D) = \infty$? A relação $\mathrm{rmi}(\cdot) \geqslant$ é definida "de baixo para cima" no caso sucessor, mas esses lemas sugerem que $\mathrm{RMI}(D) = \infty$ é uma propriedade "de cima para baixo". Estes lema e exemplo mostram como calcular $\mathrm{RMI}(D) = \infty$.

Lema 2.1.8. $\mathrm{RMI}(D) = \infty$ se e somente se existe uma árvore binária de definíveis $D_s \neq \emptyset$, s seqüência finita sobre $\{0, 1\}$, de modo que $D_\emptyset = D$, $D_{s0}, D_{s1} \subseteq D_s$ e $D_{s0} \cap D_{s1} = \emptyset$.

Demonstração: Se $\mathrm{RMI}(D) = \infty$, podemos aplicar o lema anterior indutivamente. Consideremos então a recíproca. Para cada ordinal ξ e seqüência s, mostraremos que $\mathrm{rmi}(D_s) \geqslant \xi$, podendo concluir que todos esses definíveis têm $\mathrm{RMI}(D_s) = \infty$.

Para $\xi = 0$, é fato pois $D_s \neq \emptyset$. Por indução, não há o que provar em ordinais limites; suponha então $\xi = \zeta + 1$ e que $\mathrm{rmi}(D_s) \geqslant \zeta$ para toda s. Vemos que

$$D_{s1}, D_{s01}, D_{s001}, \ldots, D_{s0\ldots01}, \ldots$$

são dois a dois disjuntos contidos em D_s, de modo que $\mathrm{rmi}(D_s) \geqslant \zeta + 1 = \xi$.

QED

Exemplo 2.1.9. Na linguagem da relação de ordem, a estrutura $\mathbb{Q}$ não tem posto: $\mathrm{RMI}(\mathbb{Q}) = \infty$. Basta tomar $D_\emptyset = \mathbb{Q}$, $D_0 =]0, \frac{1}{2}[$, $D_1 =]\frac{1}{2}, 1[$ e prosseguir subdividindo nos pontos médios dos intervalos, que são definíveis. Deve-se comparar esse resultado com o Teorema 2.3.12 e o Exemplo 2.3.7.

Consideraremos agora o posto ordinal. Este lema contrasta com o Lema 2.1.6, porque não se pode substituir ξ por ∞.

Lema 2.1.10. Se $\mathrm{RMI}(D) = \xi > \zeta$, então existem definíveis $E_n \subseteq D$, $n \in \mathbb{N}$, dois a dois disjuntos com $\mathrm{RMI}(E_n) = \zeta$.

Demonstração: Se $\xi = 0$, então não existe o ordinal ζ. Procedendo por indução em ξ, assuma $\xi > \zeta \geqslant 0$. Então $\mathrm{RMI}(D) \geqslant \zeta + 1$, existindo infinitos $D_i \subseteq D$ dois a dois disjuntos com $\mathrm{RMI}(D_i) \geqslant \zeta$ e apenas um número finito deles tem posto ξ, do contrário $\mathrm{RMI}(D) \geqslant \xi + 1$. Consideraremos os demais D_i, que podemos supor indexados D_n, $n \in \mathbb{N}$.

Temos $\zeta \leqslant \mathrm{RMI}(D_n) < \xi$. Caso $\mathrm{RMI}(D_n) = \zeta$, tome $E_n = D_n$. Se $\zeta < \mathrm{RMI}(D_n) < \xi$, por hipótese de indução existe $E_n \subseteq D_n$ com $\mathrm{RMI}(E_n) = \zeta$; de fato, existem infinitos conjuntos. Assim, E_n, $n \in \mathbb{N}$, são dois a dois disjuntos contidos em D com $\mathrm{RMI}(E_n) = \zeta$. QED

Suponha agora $\mathrm{RMI}(D) = \xi$. Chame *partição* de D, provisoriamente, a uma família de definíveis D_i, $i \in I$, dois a dois disjuntos com $\mathrm{RMI}(D_i) = \xi$ tais que $D = \bigcup_{i \in I} D_i$. Por definição, I é finito, de modo que uma partição não pode ser refinada infinitamente. Mostremos que $|I|$ é limitado.

Suponha $(D_i)_{i \in I}$ e $(E_j)_{j \in J}$ duas partições de D refinadas ao máximo, com $|I| < |J|$. Tome $S = \{(i,j) \in I \times J \mid \mathrm{RMI}(D_i \cap E_j) = \xi\}$. Como I é finito, temos $\mathrm{RMI}(E_j) = \max_{i \in I} \mathrm{RMI}(D_i \cap E_j)$ para cada $j \in J$; portanto, para todo $j \in J$ existe $i \in I$ tal que $\mathrm{RMI}(D_i \cap E_j) = \xi$. Então $|S| \geqslant |J| > |I|$. Como J é finito, temos $\mathrm{RMI}(D_i) = \max_{j \in J} \mathrm{RMI}(D_i \cap E_j)$ para cada $i \in I$; pelo mesmo raciocínio, mas com $|I| < |S|$, existem $i \in I$ e $j_1, j_2 \in J$, $j_1 \neq j_2$, tais que $\mathrm{RMI}(D_i \cap E_{j_1}) = \mathrm{RMI}(D_i \cap E_{j_2}) = \xi$. Temos $D_i \cap E_{j_2} \subseteq D_i - E_{j_1} \subseteq D_i$, donde $\mathrm{RMI}(D_i - E_{j_1}) = \xi$. Mas $D_i = (D_i \cap E_{j_1}) \cup (D_i - E_{j_1})$ definíveis disjuntos: refinamos $(D_i)_{i \in I}$, contradição.

Como (D) é uma partição de D, temos $0 < \mathrm{dMI}_{\mathfrak{A}}(D) < \omega$ nesta definição:

Definição 2.1.11. Suponha $\mathrm{RMI}_{\mathfrak{A}}(D) = \xi$. O *grau de Morley interno* de D em $\mathfrak{A}$, indicado $\mathrm{dMI}_{\mathfrak{A}}(D)$, é o máximo comprimento (finito) n de uma partição $D = D_1 \cup \ldots \cup D_n$, D_i definíveis dois a dois disjuntos com $\mathrm{RMI}_{\mathfrak{A}}(D_i) = \xi$. (Em inglês, dM abrevia *Morley degree*, novamente com a inversão francesa; escreve-se também DM, deg, Md, ...)

Note que cada D_i de uma partição refinada terá grau 1. Além disso, se $\mathrm{RMI}(D) = 0$, então $\mathrm{dMI}(D)$ é o número de elementos de D.

Obtemos uma segunda caracterização da relação $\mathrm{rmi}(\cdot) \geqslant$ no caso de ordinais sucessores, porque $\mathrm{RMI}(D) \geqslant \xi+1$ se e somente se, para $k \in \mathbb{N}^*$ arbitrariamente grande, existem definíveis $D_1, \ldots, D_k \subseteq D$ dois a dois disjuntos com $\mathrm{RMI}(D_i) \geqslant \xi$ para todo $1 \leqslant i \leqslant k$.

Proposição 2.1.12. Suponha D, E disjuntos com postos ordinais satisfazendo $\mathrm{RMI}(D) \leqslant \mathrm{RMI}(E)$. Se o posto é o mesmo, $\mathrm{dMI}(D \cup E) = \mathrm{dMI}(D) + \mathrm{dMI}(E)$; caso contrário, $\mathrm{dMI}(D \cup E) = \mathrm{dMI}(E)$.

Demonstração: Suponha que $\mathrm{RMI}(D) = \mathrm{RMI}(E)$, donde $\mathrm{RMI}(D \cup E) = \mathrm{RMI}(D) = \mathrm{RMI}(E)$. Particionando, como na definição, $D = D_1 \cup \ldots \cup D_{\mathrm{dMI}(D)}$ e $E = E_1 \cup \ldots \cup E_{\mathrm{dMI}(E)}$, observamos que $D \cup E = D_1 \cup \ldots \cup D_{\mathrm{dMI}(D)} \cup$

$E_1 \cup \ldots \cup E_{\mathrm{dMI}(E)}$ é uma partição que satisfaz as condições da definição. Então $\mathrm{dMI}(D \cup E) = \mathrm{dMI}(D) + \mathrm{dMI}(E)$.

Agora, suponha que $\mathrm{RMI}(D) < \mathrm{RMI}(E)$, donde $\mathrm{RMI}(D \cup E) = \mathrm{RMI}(E) > \mathrm{RMI}(D)$. Novamente, particione $E = E_1 \cup \ldots \cup E_{\mathrm{dMI}(E)}$ como na definição. Desta vez, observamos que $D \cup E = (D \cup E_1) \cup E_2 \cup \ldots \cup E_{\mathrm{dMI}(E)}$ é uma partição que satisfaz as condições da definição, porque $\mathrm{RMI}(E_1) = \mathrm{RMI}(E)$ e, assim, $\mathrm{RMI}(D \cup E_1) = \mathrm{RMI}(E)$. Então $\mathrm{dMI}(D \cup E) = \mathrm{dMI}(E)$. QED

Corolário 2.1.13. (i) Por indução, se $D_1, \ldots, D_n \in \mathrm{Def}_A^m$, $n \geqslant 1$, são dois a dois disjuntos com mesmo posto interno ordinal, então $\mathrm{dMI}(D_1 \cup \ldots \cup D_n) = \sum_{i=1}^n \mathrm{dMI}(D_i)$.

(ii) Se $D \subseteq E$ com o mesmo posto interno ordinal, então $\mathrm{dMI}(D) \leqslant \mathrm{dMI}(E)$, bastando particionar $E = (E - D) \cup D$.

Concluímos a exposição sobre o posto interno com alguns resultados muito úteis.

Proposição 2.1.14. RMI e dMI são invariantes por bijeções definíveis (na mesma estrutura) e isomorfismos.

Demonstração: Entendem-se as bijeções como parciais, ou seja, são bijeções entre seus domínios e suas imagens. Por exemplo, se $a \in A^k$ é fixado, a função $f : A^m \to A^{m+k}$, $f(x) = (x, a)$, é definível e induz uma bijeção ente D e $D \times \{a\}$. Também permutações de coordenadas são bijeções definíveis.

Lembramos que imagens diretas e inversas de definíveis por funções definíveis são também definíveis. Resta observar, portanto, que bijeções preservam partições, sejam infinitas (definição de $\mathrm{rmi}(\cdot) \geqslant$) ou finitas (definição de dMI). O mesmo raciocínio aplica-se a isomorfismos. QED

Proposição 2.1.15. Um definível D é minimal se e somente se $\mathrm{RMI}(D) = 1$ e $\mathrm{dMI}(D) = 1$.

Demonstração: Lembramos que posto $\geqslant 1$ é prerrogativa de definíveis infinitos. Se $\mathrm{RMI}(D) = \mathrm{dMI}(D) = 1$, então D é infinito, mas não se particiona em dois definíveis infinitos, ou seja, é minimal. Se D é minimal, por definição $\mathrm{RMI}(D) \geqslant 1$. Se fosse $\mathrm{RMI}(D) \geqslant 2$, haveria uma família infinita de definíveis com posto $\geqslant 1$, portanto infinitos, dois a dois disjuntos contidos em D, absurdo. Então $\mathrm{RMI}(D) = 1$ e, analogamente, $\mathrm{dMI}(D) = 1$. QED

Lema 2.1.16. Se $\mathfrak{A} \prec \mathfrak{B}$ e $D \in \mathrm{Def}^m_{\mathfrak{A},A}$, $E \in \mathrm{Def}^m_{\mathfrak{B},B}$ com $D \subseteq E$, então $\mathrm{RMI}_{\mathfrak{A}}(D) \leqslant \mathrm{RMI}_{\mathfrak{B}}(E)$ e, sendo o mesmo posto ordinal, $\mathrm{dMI}_{\mathfrak{A}}(D) \leqslant \mathrm{dMI}_{\mathfrak{B}}(E)$. Em particular, se ϕ é uma fórmula de $\mathrm{L}(A)$, então $\mathrm{RMI}_{\mathfrak{A}}(\phi(\mathfrak{A})) \leqslant \mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B}))$.

Demonstração: Basta provar que se $\mathrm{RMI}_{\mathfrak{A}}(D) \geqslant \xi$ então $\mathrm{RMI}_{\mathfrak{B}}(E) \geqslant \xi$ por indução em ξ, independentemente dos definíveis. Se ξ é um ordinal limite, mesmo 0, segue por definição das relações $\mathrm{rmi}_{\mathfrak{A}}(\cdot)\geqslant$ e $\mathrm{rmi}_{\mathfrak{B}}(\cdot)\geqslant$. Concentremo-nos então no caso sucessor $\xi = \zeta + 1$.

Se ϕ_i, $i \in I$, são fórmulas de $\mathrm{L}(A)$ tais que $\phi_i(\mathfrak{A})$ formam uma família infinita de A-definíveis dois a dois disjuntos contidos em D com $\mathrm{RMI}_{\mathfrak{A}}(\phi_i(\mathfrak{A})) \geqslant \zeta$, então também $\phi_i(\mathfrak{B}) \cap E$ são infinitos definíveis dois a dois disjuntos contidos em E e tais que $\mathrm{RMI}_{\mathfrak{B}}(\phi_i(\mathfrak{B}) \cap E) \geqslant \zeta$ por hipótese de indução. Mais precisamente, $\phi_i(\mathfrak{A}) \subseteq \phi_i(\mathfrak{B})$ por extensão elementar e $\phi_i(\mathfrak{A}) \subseteq D \subseteq E$ implicam $\phi_i(\mathfrak{A}) \subseteq \phi_i(\mathfrak{B}) \cap E$. Assim, $\mathrm{RMI}_{\mathfrak{B}}(E) \geqslant \mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B}) \cap E) \geqslant \zeta + 1 = \xi$.

Considere agora a situação $\mathrm{RMI}_{\mathfrak{A}}(D) = \mathrm{RMI}_{\mathfrak{B}}(E) = \xi$. Suponha I finito e $\mathrm{RMI}_{\mathfrak{A}}(\phi_i(\mathfrak{A})) = \xi$: obtemos $\mathrm{RMI}_{\mathfrak{B}}(\phi_i(\mathfrak{B}) \cap E) = \xi$, de modo que $|I| \leqslant \mathrm{dMI}_{\mathfrak{B}}(E)$. QED

Agora, definiremos o posto de Morley "geral" com ajuda de extensões ω-saturadas. Precisamos de um lema; começamos por lembrar que

Fato 2.1.17. Toda estrutura tem uma extensão elementar ω-saturada.

Demonstração: Tome um cardinal regular $\kappa > |\mathrm{L}|$. Pelo Teorema 1.4.11, toda estrutura tem uma extensão elementar κ-grande. Vimos também que essa extensão é, portanto, κ-saturada. Como $\omega \leqslant \kappa$, a extensão é ω-saturada por definição.

Há modos muito menos dispendiosos de mostrá-lo, encontrados em nossas referências costumeiras. QED

Encontramos no Lema 7.1.20 de [Chang, Keisler] o melhor enunciado para nossos propósitos:

Lema 2.1.18. Suponha $\mathfrak{B}, \mathfrak{C}$ duas L-estruturas ω-saturadas, $X \subseteq B, C$ com $(\mathfrak{B}, (x)_{x\in X}) \equiv (\mathfrak{C}, (x)_{x\in X})$ e ϕ uma fórmula de $\mathrm{L}(X)$. Então $\mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B})) = \mathrm{RMI}_{\mathfrak{C}}(\phi(\mathfrak{C}))$ e, caso seja um posto ordinal, também $\mathrm{dMI}_{\mathfrak{B}}(\phi(\mathfrak{B})) = \mathrm{dMI}_{\mathfrak{C}}(\phi(\mathfrak{C}))$.

Demonstração: Provaremos por indução em ξ que se $\mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B})) = \xi$ então $\mathrm{RMI}_{\mathfrak{C}}(\phi(\mathfrak{C})) = \xi$, independentemente de $\mathfrak{B}, \mathfrak{C}, X, \phi$. (Por simetria, portanto, vale a recíproca de $\mathfrak{C}$ para $\mathfrak{B}$ e a igualdade também para os "postos" -1, caso simples do vazio, e ∞.) Assuma que a propriedade vale para ordinais $< \xi$ e que $\mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B})) = \xi$. Permutando $\mathfrak{B}$ e $\mathfrak{C}$, vemos que não pode ocorrer $\mathrm{RMI}_{\mathfrak{C}}(\phi(\mathfrak{C})) < \xi$, donde $\mathrm{RMI}_{\mathfrak{C}}(\phi(\mathfrak{C})) \geqslant \xi$.

Sejam $\phi_i(v, w_i)$, $i \in I$, fórmulas de L com v, w_i seqüências de m, n_i variáveis respectivamente, e $c_i \in C^{n_i}$ de modo que $\phi_i(\mathfrak{C}, c_i)$ sejam dois a dois disjuntos contidos em $\phi(\mathfrak{C})$ com posto $\geqslant \xi$. Seja ainda x a n-upla de parâmetros de X em ϕ. Suponha que $|I| \geqslant k > \mathrm{dMI}_{\mathfrak{B}}(\phi(\mathfrak{B}))$: chegaremos a uma contradição. Para simplificar a notação, assuma $1, \ldots, k \in I$. Como $\mathfrak{B}$ é ω-saturada e $(\mathfrak{B}, x) \equiv (\mathfrak{C}, x)$, podemos aplicar o Lema 1.4.3 $n_1 \ldots n_k$ vezes para obter $b_1 \in B^{n_1}, \ldots, b_k \in B^{n_k}$ tais que

$$(\mathfrak{B}, x, b_1, \ldots, b_k) \equiv (\mathfrak{C}, x, c_1, \ldots, c_k) .$$

Essa equivalência mostra que $\phi_i(\mathfrak{B}, b_i)$, $1 \leqslant i \leqslant k$, são definíveis dois a dois disjuntos contidos em $\phi(\mathfrak{B})$. Pela hipótese de indução aplicada a essa equivalência, se algum $\phi_i(\mathfrak{B}, b_i)$ tivesse posto $< \xi$, então $\phi_i(\mathfrak{C}, c_i)$ teria posto $< \xi$, mas todos têm posto $\geqslant \xi$, contradição.

Assim, $|I| \leqslant \mathrm{dMI}_{\mathfrak{B}}(\phi(\mathfrak{B}))$, o que dá igualdade de posto (I não pode ser infinito) e então de grau (podemos tomar $|I| = \mathrm{dMI}_{\mathfrak{C}}(\phi(\mathfrak{C}))$ e obter a igualdade por simetria). QED

Assim, esta definição independe da extensão tomada:

Definição 2.1.19. Suponha ϕ uma fórmula de $\mathrm{L}(A)$. Seja $\mathfrak{B}$ uma extensão elementar ω-saturada de $\mathfrak{A}$. Definimos os *posto e grau de Morley* do definível $\phi(\mathfrak{A})$ como $\mathrm{RM}_{\mathfrak{A}}(\phi(\mathfrak{A})) = \mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B}))$ e, caso esse seja um ordinal, $\mathrm{dM}_{\mathfrak{A}}(\phi(\mathfrak{A})) = \mathrm{dMI}_{\mathfrak{B}}(\phi(\mathfrak{B}))$.

Usualmente, escreve-se apenas $\mathrm{RM}_{\mathfrak{A}}(\phi)$ e $\mathrm{dM}_{\mathfrak{A}}(\phi)$. A definição que apresentamos é dada em [Marker], mas os Lemas 2.1.16 e 2.1.18 mostram que equivale à de [Hodges] do supremo

$$\mathrm{RM}_{\mathfrak{A}}(\phi(\mathfrak{A})) = \sup_{\mathfrak{A} \prec \mathfrak{B}} \mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B}))$$

sobre uma classe própria de extensões e que é, de fato, um máximo.

Do mesmo modo, se $\mathfrak{A} \prec \mathfrak{B}$ e ϕ é uma fórmula com parâmetros em A, então $\mathrm{RM}_{\mathfrak{A}}(\phi(\mathfrak{A})) = \mathrm{RM}_{\mathfrak{B}}(\phi(\mathfrak{B}))$ e, no caso ordinal, $\mathrm{dM}_{\mathfrak{A}}(\phi(\mathfrak{A})) = \mathrm{dM}_{\mathfrak{B}}(\phi(\mathfrak{B}))$, bastando considerar uma extensão ω-saturada elementar de $\mathfrak{B}$, que o será também de $\mathfrak{A}$. Essa propriedade faz o posto de Morley mais útil que o interno.

Finalmente, mas imediatamente, vemos que por definição os postos de Morley geral e interno coincidem em estruturas ω-saturadas. Por comparação com o posto interno em uma extensão ω-saturada, obtemos o

Teorema 2.1.20. Para $\mathfrak{A}$ uma L-estrutura arbitrária e $D, E \in \mathrm{Def}^m_{\mathfrak{A},A}$, valem:

(i) $\mathrm{RM}(D) \geqslant 0 \Leftrightarrow D \neq \emptyset$; $\mathrm{RM}(D) = 0 \Leftrightarrow D$ é finito não-vazio, caso em que $\mathrm{dM}(D) = |D|$.

(ii) $\mathrm{RM}(D \cup E) = \max\{\mathrm{RM}(D), \mathrm{RM}(E)\}$.

(iii) Se $D \subseteq E$ então $\mathrm{RM}(D) \leqslant \mathrm{RM}(E)$ e, caso o posto seja o mesmo ordinal, $\mathrm{dM}(D) \leqslant \mathrm{dM}(E)$.

(iv) Suponha D, E disjuntos com $-1 < \mathrm{RM}(D) \leqslant \mathrm{RM}(E) < \infty$. Então, se D e E têm mesmo posto, $\mathrm{dM}(D \cup E) = \mathrm{dM}(D) + \mathrm{dM}(E)$; caso contrário, $\mathrm{dM}(D \cup E) = \mathrm{dM}(E)$.

(v) $\mathrm{RM}_{\mathfrak{A}}$ e $\mathrm{dM}_{\mathfrak{A}}$ são invariantes por bijeções definíveis e isomorfismos.

Demonstração: Provemos (i). Suponha que ϕ seja uma fórmula de $\mathrm{L}(A)$ com $D = \phi(\mathfrak{A})$ e $\mathfrak{B}$ uma extensão elementar ω-saturada de $\mathfrak{A}$. Temos: $D \neq \emptyset \Leftrightarrow \mathfrak{A} \models \exists v\, \phi(v) \Leftrightarrow \mathfrak{B} \models \exists v\, \phi(v) \Leftrightarrow \phi(\mathfrak{B}) \neq \emptyset \Leftrightarrow \mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B})) \geqslant 0$. No caso finito, temos $|\phi(\mathfrak{A})| = |\phi(\mathfrak{B})|$.

As afirmações (ii), (iii) e (iv) podendo ser verificadas de modo análogo, observamos os cuidados necessários para estabelecer (v). Considerando as fórmulas de $\mathrm{L}(A)$ envolvidas, basta seguir a elementaridade da extensão para vermos que a função definível continua função, com domínio e imagem apropriados e ainda bijeção. Pode-se então proceder à comparação na extensão. QED

Proposição 2.1.21. Um definível D é fortemente minimal se e somente se $\mathrm{RM}(D) = 1$ e $\mathrm{dM}(D) = 1$.

Demonstração: Seja ϕ uma fórmula de $\mathrm{L}(A)$ tal que $D = \phi(\mathfrak{A})$.

Suponha D fortemente minimal e tome $\mathfrak{C}$ uma extensão elementar ω-saturada de $\mathfrak{A}$. Temos $\phi(\mathfrak{C})$ minimal em $\mathfrak{C}$ por definição, de modo que $\mathrm{RM}_{\mathfrak{A}}(\phi(\mathfrak{A})) = \mathrm{RMI}_{\mathfrak{C}}(\phi(\mathfrak{C})) = 1$ e $\mathrm{dM}_{\mathfrak{A}}(\phi(\mathfrak{A})) = \mathrm{dMI}_{\mathfrak{C}}(\phi(\mathfrak{C})) = 1$.

Suponha agora $\mathrm{RM}(D) = \mathrm{dM}(D) = 1$ e $\mathfrak{A} \prec \mathfrak{B}$ arbitrária: devemos mostrar que $\phi(\mathfrak{B})$ é minimal em $\mathfrak{B}$. Tome $\mathfrak{C}$ uma extensão elementar ω-saturada de $\mathfrak{B}$. Temos $\mathrm{RMI}_{\mathfrak{A}}(\phi(\mathfrak{A})) \leqslant \mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B})) \leqslant \mathrm{RMI}_{\mathfrak{C}}(\phi(\mathfrak{C})) = \mathrm{RM}_{\mathfrak{A}}(\phi(\mathfrak{A})) = 1$ e, como esses postos são ordinais, podemos calcular $\mathrm{dMI}_{\mathfrak{A}}(\phi(\mathfrak{A})) \leqslant \mathrm{dMI}_{\mathfrak{B}}(\phi(\mathfrak{B})) \leqslant \mathrm{dMI}_{\mathfrak{C}}(\phi(\mathfrak{C})) = \mathrm{dM}_{\mathfrak{A}}(\phi(\mathfrak{A})) = 1$. Obtemos automaticamente $\mathrm{dMI}_{\mathfrak{B}}(\phi(\mathfrak{B})) = 1$. Como D é infinito, temos $\mathrm{RMI}_{\mathfrak{A}}(\phi(\mathfrak{A})) \geqslant 1$ e vem $\mathrm{RMI}_{\mathfrak{B}}(\phi(\mathfrak{B})) = 1$. QED

Exemplo 2.1.22. Como ACF é fortemente minimal, todo corpo algebricamente fechado tem posto e grau de Morley (gerais ou internos) iguais a 1.

Chame um X-definível com posto ξ de *irredutível (sobre X)* se não é a união de dois X-definíveis disjuntos de posto ξ. (Comentamos que havíamos derivado essa nomenclatura de modo óbvio, mas viemos a encontrá-la na pág. 498 de [Chang, Keisler].) *Atenção: diferentemente dos irredutíveis topológicos que definiremos na Seção 6.1, a condição de disjunção é essencial.*

Um definível particiona-se, por seu grau de Morley, em definíveis com grau 1 com parâmetros que não controlamos, possivelmente apenas em uma extensão ω-saturada. Porém, o mesmo raciocínio permite-nos ainda particionar $D \in$

Def^m_X em outros X-definíveis dois a dois disjuntos $D_1, \ldots, D_n$ de mesmo posto e irredutíveis, embora apenas possa-se garantir $\mathrm{dM}(D_i) \geqslant 1$ e $1 \leqslant n \leqslant \mathrm{dM}(D)$. O raciocínio que fizemos para limitar o tamanho de uma partição também vale nessa situação, para mostrar que n é único.

Apresentamos agora uma notação para uso futuro, mas que também parafraseia alguns resultados. Suponha $D, E, F \in \mathrm{Def}^m_{\mathfrak{A},A}$.

Proposição 2.1.23. A relação $=_\xi$ definida por

$$D =_\xi E \Leftrightarrow \mathrm{RM}(D \triangle E) < \xi ,$$

onde $D \triangle E = (D - E) \cup (E - D)$, é uma relação de equivalência em $\mathrm{Def}^m_{\mathfrak{A},A}$. A relação $\subseteq_\xi$ definida por

$$D \subseteq_\xi E \Leftrightarrow \mathrm{RM}(D - E) < \xi$$

induz uma relação de ordem parcial no conjunto quociente de $=_\xi$ com a qual o chamaremos simplesmente a álgebra quociente de $=_\xi$. Note que se $D \subseteq E$ então $D \subseteq_\xi E$.

Demonstração: Primeiramente, notamos que $D \triangle D = \emptyset$, de modo que $\mathrm{RM}(D \triangle D) = -1 < \xi$. Também temos $D \triangle E = E \triangle D$. Aplicando o teorema a $D \triangle F \subseteq (D \triangle E) \cup (E \triangle F)$, concluímos que $=_\xi$ é uma relação de equivalência.

Suponha agora que $D =_\xi E$: então $D \subseteq_\xi E$, já que $D - E \subseteq D \triangle E$. Se $D \subseteq_\xi E$ e $E \subseteq_\xi D$, então $\mathrm{RM}(D - E), \mathrm{RM}(E - D) < \xi$, donde $\mathrm{RM}(D \triangle E) < \xi$ e $D =_\xi E$. Finalmente, se $D \subseteq_\xi E$ e $E \subseteq_\xi F$, então $D \subseteq_\xi F$, pois $D - F \subseteq (D - E) \cup (E - F)$. QED

Observamos que, tanto no enunciado como na demonstração, ξ pode ser substituído por ∞.

Contudo, para ξ ordinal, trata-se de uma álgebra atômica, em que os átomos são as classes de equivalência dos definíveis irredutíveis de posto ξ.

Corolário 2.1.24. Se $\mathrm{RM}(D) = \mathrm{RM}(E) = \xi$ e $D \subseteq E$ então $\mathrm{dM}(D) \leqslant \mathrm{dM}(E)$, com igualdade se e somente se $D =_\xi E$.

Demonstração: Temos $D =_\xi E \Leftrightarrow E \subseteq_\xi D$. Se $\mathrm{RM}(E - D) < \xi$ então $\mathrm{dM}(E) = \mathrm{dM}(D)$. Se $\mathrm{RM}(E - D) = \xi$ então $\mathrm{dM}(E) = \mathrm{dM}(E - D) + \mathrm{dM}(D)$, que são dois números não-nulos, donde $\mathrm{dM}(E) > \mathrm{dM}(D)$. QED

2.2. Posto de Morley para tipos

Fixe novamente uma L-estrutura $\mathfrak{A}$, e também $X \subseteq A$. Por toda a seção, $D, E \in \mathrm{Def}^m_X$ e $p, q \in S_m(X)$. Trabalharemos com $p \in S_m(X)$ concebido como ultrafiltro em Def^m_X, com a devida atenção em extensões elementares.

Definição 2.2.1. Defina o *posto de Morley* $\mathrm{RM}_{\mathfrak{A}}(p) = \min\{\mathrm{RM}_{\mathfrak{A}}(D) \mid D \in p\}$. Note que, se p não contém um definível com posto, $\mathrm{RM}_{\mathfrak{A}}(p) = \infty$ e diz-se que p *não tem posto*; sempre $\mathrm{RM}_{\mathfrak{A}}(p) \geqslant 0$ pois seus definíveis são não-vazios; é efetivamente mínimo pela boa ordem dos ordinais.

Caso $\mathrm{RM}_{\mathfrak{A}}(p) < \infty$, dentre os definíveis de p com posto $\mathrm{RM}_{\mathfrak{A}}(p)$ há um ou mais com grau mínimo n: defina o *grau de Morley* $\mathrm{dM}_{\mathfrak{A}}(p) = n$.

Por exemplo, suponha que $p \subseteq q$ são tipos, sobre conjuntos um incluso no outro: a definição por mínimo dá $\mathrm{RM}(p) \geqslant \mathrm{RM}(q)$ e, caso os postos sejam iguais, também $\mathrm{dM}(p) \geqslant \mathrm{dM}(q)$.

Dados $a_1, \ldots, a_m \in A$, para evitar excesso de parênteses escreve-se

$$\mathrm{RM}(a_1, \ldots, a_m/X) = \mathrm{RM}(t((a_1, \ldots, a_m)/X))$$

e analogamente com dM.

Assim, para $a \in A^m$ e $X \subseteq Y \subseteq A$, temos $\mathrm{RM}(a/Y) \leqslant \mathrm{RM}(a/X)$ e no caso de igualdade a relação transfere-se para o grau dos tipos. É mais freqüente o caso específico de $b \in A^n$ e $\mathrm{RM}(a/Xb) \leqslant \mathrm{RM}(a/X)$. Também temos a

Proposição 2.2.2. Sejam $a \in A^m$, $b \in B^n$ com $m, n \neq 0$: então $\mathrm{RM}(a/X) \leqslant \mathrm{RM}(a, b/X)$. Em geral, por permutações $\emptyset$-definíveis, podemos supor os elementos a_i, b_j em qualquer seqüência.

Referência: O Exercício 6.6.11 de [Marker].

Apresentamos a demonstração da relação mais simples $\mathrm{RM}(a/Xb) \leqslant \mathrm{RM}(a, b/X)$. Por definição, existe $D \in \mathrm{Def}_X^{m+n}$ com $(a, b) \in D$ e $\mathrm{RM}(a, b/X) = \mathrm{RM}(D)$. Tome $\Delta = \{\alpha \in A^m \mid (\alpha, b) \in D\}$ conjunto Xb-definível. Δ tem o mesmo posto de $\Delta \times \{b\}$ pois $f : \Delta \to \Delta \times \{b\}$, $f(\alpha) = (\alpha, b)$, é uma bijeção definível. Como $\Delta \times \{b\} \subseteq D$, temos $\mathrm{RM}(\Delta) = \mathrm{RM}(\Delta \times \{b\}) \leqslant \mathrm{RM}(D)$. Já que $a \in \Delta$, vem $\mathrm{RM}(a/Xb) \leqslant \mathrm{RM}(a, b/X)$.

Observamos anteriormente que os posto e grau de Morley do definível de uma fórmula fixada é invariante sob extensões elementares. Assim, para $\mathfrak{A} \prec \mathfrak{B}$ e $p \in S_m^{\mathfrak{A}}(X) = S_m^{\mathfrak{B}}(X)$, temos $\mathrm{RM}_{\mathfrak{A}}(p) = \mathrm{RM}_{\mathfrak{B}}(p)$ e $\mathrm{dM}_{\mathfrak{A}}(p) = \mathrm{dM}_{\mathfrak{B}}(p)$.

É preciso tomar cuidado com a definição de RM, feita para definíveis em Def_A^m, enquanto $p \subseteq \mathrm{Def}_X^m$, sendo a principal razão a dificuldade apontada na discussão sobre partição.

Suponha que $\mathrm{RM}(p) = \xi$. Por definição, existe $D \in p$ com $\mathrm{RM}(D) = \xi$ e $\mathrm{dM}(D) = \mathrm{dM}(p)$, e diz-se que p *determina* D porque, se $E \in p$ também satisfaz $\mathrm{RM}(E) = \xi$ e $\mathrm{dM}(E) = \mathrm{dM}(p)$, então $D =_\xi E$. De fato, como $D \cap E \in p$, vale $\mathrm{RM}(D \cap E) \geqslant \mathrm{RM}(p)$, donde se conclui $\mathrm{RM}(D \cap E) = \xi$. Também $\mathrm{dM}(D \cap E) \geqslant$

$\mathrm{dM}(p)$, donde $\mathrm{dM}(D \cap E) = \mathrm{dM}(D)$. Sabemos que $\mathrm{RM}(D - E) \leqslant \mathrm{RM}(D) = \xi$. Se $\mathrm{RM}(D - E) = \xi$ então $\mathrm{dM}(D - E) = 0$, absurdo. Assim, $\mathrm{RM}(D - E) < \xi$; analogamente, $E \subseteq_\xi D$.

Por outro lado, se $E =_\xi D$ então $E \in p$. Basta observar que, como $\mathrm{RM}(D \triangle E) < \xi$, $D \triangle E \notin p$. Mas $D \cup E \in p$, pois contém D, e é a união de $D \triangle E$ e $D \cap E$ disjuntos. Assim, $D \cap E \in p$.

Particione agora $D = D_1 \cup \ldots \cup D_n$, cada $D_i \in \mathrm{Def}_X^m$ irredutível de posto ξ. Algum $D_i \in p$ porque este é um ultrafiltro, mas então $\mathrm{dM}(D_i) \geqslant \mathrm{dM}(p)$ por minimalidade, de modo que $n = 1$. Isso nos permite concluir que D é irredutível; em particular, se p é global ($X = A$) e $\mathfrak{A}$ é ω-saturada, D tem grau 1 e $\mathrm{dM}(p) = 1$.

O Exercício 5.6.10 de [Hodges] sugere tomar, para cada d, uma estrutura de relação de equivalência com d classes infinitas para obter tipos sobre $\emptyset$ com posto 1 e grau d. Quanto a tipos globais, obteremos na Seção 2.4 condições aplicáveis para grau 1.

Lema 2.2.3. Se $p, q \in S_m(X)$ são tipos distintos com posto e determinam $D, E \in S_m(X)$ respectivamente, então $D \neq E$.

Demonstração: Existe $F \in \mathrm{Def}_X^m$ tal que $F \in p$, $F \notin q$ (ou, tomando-se o complemento, $F \in q$, $F \notin p$). Então $\mathrm{RM}(D \cap F) \leqslant \mathrm{RM}(D) = \mathrm{RM}(p)$ e $\mathrm{RM}(E - F) \leqslant \mathrm{RM}(E) = \mathrm{RM}(q)$. Mas $D \cap F \in p$ e $E - F \in q$; por minimalidade, $\mathrm{RM}(D \cap F) = \mathrm{RM}(D)$ e $\mathrm{RM}(E - F) = \mathrm{RM}(E)$. Se $D = E$, temos $\mathrm{RM}(D \cap F) = \mathrm{RM}(D) = \mathrm{RM}(D - F)$, de modo que $\mathrm{dM}(D \cap F) < \mathrm{dM}(D) = \mathrm{dM}(p)$, contradição. QED

Reciprocamente, D irredutível *determina* p do seguinte modo:

Proposição 2.2.4. Se $\mathrm{RM}(D) = \xi$ e D é irredutível, então $p = \{E \in \mathrm{Def}_X^m \mid D \subseteq_\xi E\}$ é o único tipo em $S_m(X)$ com posto ξ e grau $\mathrm{dM}(D)$ que contém D — note que, assim, p determina D.

Demonstração: A unicidade é dada pelo lema, já que p determinará D.

Começamos por verificar que p é um filtro. Se $E \in p$ e $E \subseteq F \in \mathrm{Def}_X^m$, então $D \subseteq_\xi E \subseteq_\xi F$ e $F \in p$. Se $E, F \in p$, então $\mathrm{RM}(D - E), \mathrm{RM}(D - F) < \xi$ e vem $\mathrm{RM}(D - (E \cap F)) < \xi$, donde $E \cap F \in p$. É claro que $\emptyset \notin p$, porque $\mathrm{RM}(D) = \xi$, de modo que p é próprio, e que $D \in p$.

Queremos que p seja um ultrafiltro. Se $E, A^m - E \in p$, obtemos $\emptyset \in p$, contradição. Se $E, A^m - E \notin p$, temos $\mathrm{RM}(D - E) \geqslant \xi$ e $\mathrm{RM}(D \cap E) = \mathrm{RM}(D - (A^m - E)) \geqslant \xi$; então $\mathrm{RM}(D \cap E) = \mathrm{RM}(D - E) = \mathrm{RM}(D)$, donde $\mathrm{dM}(D) = \mathrm{dM}(D \cap E) + \mathrm{dM}(D - E)$, contradizendo a irredutibilidade de D.

Suponha agora que p determine D' como acima. Então $\mathrm{RM}(D') \leqslant \mathrm{RM}(D) = \xi$, mas $D \subseteq_\xi D'$, de modo que $\mathrm{RM}(D \cap D') = \xi$ e então $\mathrm{RM}(D') = \xi$. Também $\mathrm{dM}(D') \leqslant \mathrm{dM}(D)$ e novamente $D \subseteq_\xi D'$ implica $\mathrm{dM}(D') = \mathrm{dM}(D)$. Concluímos que p tem o posto e o grau de D. QED

Agora, deduziremos importantes relações duais às definições e que, com estas, sugerimos chamar *equações de posto*:

Proposição 2.2.5 (Equações de posto). Suponha $D \in \mathrm{Def}^m_X$ não-vazio e considere o espaço $S_m(X)$.

(Lembre que $\mathrm{RM}(p) = \min_{D\in p}\mathrm{RM}(D)$ e, caso o posto seja um ordinal, $\mathrm{dM}(p) = \min \mathrm{dM}(D)$ com $D \in p$ e $\mathrm{RM}(D) = \mathrm{RM}(p)$.)

Então $\mathrm{RM}(D) = \max_{p\in\langle D\rangle} \mathrm{RM}(p)$ e, caso o posto seja um ordinal, $\mathrm{dM}(D) = \sum \mathrm{dM}(p)$ com $p \in \langle D\rangle$ e $\mathrm{RM}(p) = \mathrm{RM}(D)$.

Demonstração: Se $D \neq \emptyset$, sempre existe $p \in \langle D\rangle$ e $\mathrm{RM}(p) \leqslant \mathrm{RM}(D)$ por definição. Se $\mathrm{RM}(D) = \infty$, imitamos o raciocínio anterior. Tome $\mathscr{F} = \{E \in \mathrm{Def}^m_X \mid D - E$ tem posto ordinal ou -1, ou seja, $D \subseteq_\infty E\}$. Novamente, $\mathscr{F}$ é um filtro próprio que contém D. O raciocínio não se aplica para mostrar que $\mathscr{F}$ é ultrafiltro, mas $\mathscr{F}$ estende-se a um ultrafiltrp p. Suponha que $E \in p$ tenha posto ordinal. Então $D \cap E \in p$ tem posto ordinal, mas $D - (D - E) = D \cap E$, de modo que $D - E \in \mathscr{F} \subseteq p$, contradição. Obtemos $\mathrm{RM}(p) = \infty$ máximo.

Suponha então que D tem posto ordinal. Particione $D = D_1 \cup \ldots \cup D_n$ em Def^m_X com D_i irredutíveis. D_1 determina um tipo p, que contém D e com $\mathrm{RM}(p) = \mathrm{RM}(D_1) = \mathrm{RM}(D)$ máximo. Também temos $\mathrm{dM}(D) = \sum_{i=1}^n \mathrm{dM}(D_i)$. Cada D_i determina um tipo p_i, bastando então mostrar que $p_1, \ldots, p_n$ são todos os tipos contendo D e com posto $\mathrm{RM}(D)$. Um outro tipo p com essas propriedades conteria algum D_i por ser ultrafiltro. Suponha que p determine D'. Então $D' \cap D_i \in p$ e também é determinado por p, mas $D' \cap D_i \subseteq D_i$ irredutível, donde $\mathrm{dM}(p) = \mathrm{dM}(D' \cap D_i) = \mathrm{dM}(D_i)$ e $p = p_i$. QED

Apresentamos, agora, a caracterização topológica do posto de Morley de um tipo, ou melhor, a definição original do próprio Morley em seu artigo *Categoricity in power*, Transactions AMS, vol. 114, no. 2, 1965, p. 514–538. Os enunciados destas proposições correspondem ao caso sucessor de uma definição por recursão transfinita.

Não faremos uso futuro deste material, que encerra esta seção. Por conveniência, escreva $\mathrm{RMI}(p) = \min_{D\in p} \mathrm{RMI}(D)$.

Proposição 2.2.6. $\mathrm{RMI}(p) \geqslant \xi + 1$ se e somente se, para cada $D \in p$, existem tipos globais distintos $p_i \in \langle D\rangle \subseteq S_m(A)$, $i \in \mathbb{N}$, com $\mathrm{RMI}(p_i) \geqslant \xi$.

Demonstração: Para a implicação direta, fixe $D \in p$ com $\mathrm{RMI}(D) \gg \xi + 1$. Então existem definíveis $D_i \subseteq D$, $i \in \mathbb{N}$, dois a dois disjuntos com $\mathrm{RMI}(D_i) \geqslant \xi$. Note que sabemos apenas que $D_i \in \mathrm{Def}_A^m$, o que nos força a trabalhar em $S_m(A)$. O mesmo raciocínio com que provamos a Proposição 2.2.5 mostra que cada $\langle D_i \rangle$ contém um tipo p_i com $\mathrm{RMI}(p_i) = \mathrm{RMI}(D_i)$ máximo. Esses tipos são distintos porque $D_i \cap D_j = \emptyset$ para $i \neq j$ e pertencem a $\langle D \rangle$ porque cada $D_i \subseteq D$.

Para a recíproca, fixe $D \in p$ arbitrário e assuma a condição no enunciado: ao mostrarmos que $\mathrm{RMI}(D) \geqslant \xi + 1$, obtemos $\mathrm{RMI}(p) \geqslant \xi + 1$. Suponha então $\mathrm{RMI}(D) \leqslant \xi$: como $D \in p_i$ e $\mathrm{RMI}(p_i) \geqslant \xi$, temos $\mathrm{RMI}(D) = \mathrm{RMI}(p_i) = \xi$. Novamente, o raciocínio que demonstrou as equações de posto mostraria $\mathrm{dMI}(D) = \sum \min_{E \in q} \mathrm{dMI}(E)$ com $q \in \langle D \rangle$ e $\mathrm{RMI}(q) = \mathrm{RMI}(D)$. Como os tipos p_i são em número infinito, obtemos uma contradição com $\mathrm{dMI}(D) < \omega$.

QED

Se $X = A$, ou seja, p é um tipo global, então trabalhamos em $S_m(A)$ e $\mathrm{RMI}(p) \geqslant \xi + 1$ se e somente se p é ponto de acumulação do conjunto dos tipos q com $\mathrm{RMI}(q) \geqslant \xi$. De fato, se p é ponto de acumulação, qualquer vizinhança $\langle D \rangle$ de p contém um tal q e, pela propriedade de Hausdorff e por indução, um número infinito desses tipos.

Façamos, portanto, uma digressão topológica. Seja S um espaço topológico compacto Hausdorff. Para $R \subseteq S$, defina a *derivada de Cantor–Bendixson* $R' = \{p \in R \mid p \text{ não é ponto isolado de } R\}$. Note que $R' \subseteq R$, de modo que é adequada a intersecção nesta definição por recursão transfinita: $S^{(0)} = S$; $S^{(\xi+1)} = (S^{(\xi)})'$; $S^{(\lambda)} = \bigcap_{\xi<\lambda} S^{(\xi)}$ se λ é limite > 0. Verifica-se que cada $S^{(\xi)}$ é um subconjunto fechado de S e que existe um ordinal ζ tal que $S^{(\xi)} = S^{(\zeta)}$ para todo $\xi \geqslant \zeta$. Denota-se $S^{(\infty)} = S^{(\zeta)}$ e vê-se que $S^{(\infty)}$ não tem pontos isolados, sendo de fato a união dos subconjuntos de S que não têm pontos isolados. Por ζ ser o primeiro ordinal para o qual $S^{(\zeta+1)} = S^{(\zeta)}$, obtemos

$$S = \bigcup_{\xi<\zeta} (S^{(\xi)} - S^{(\xi+1)}) \cup S^{(\infty)}$$

ou $S = S^{(\infty)}$ se $\zeta = 0$. Note que essas componentes são duas a duas disjuntas.

Definição 2.2.7. O *posto de Cantor–Bendixson* de $p \in S$, se existir, é o ordinal $\mathrm{CB}(p) = \xi$ para o qual $p \in S^{(\xi)} - S^{(\xi+1)}$, ou seja, p é um ponto isolado de $S^{(\xi)}$. Caso não exista um tal ordinal, escreve-se $\mathrm{CB}(p) = \infty$.

Então $S^{(\xi)} = \{p \in S \mid \mathrm{CB}(p) \geqslant \xi\}$ e $\mathrm{CB}(p) \geqslant \xi + 1$ se e somente se p é ponto de acumulação de $S^{(\xi)}$.

Vemos assim que RMI(p) e CB(p) coincidem em $S_m(A)$, o que é usado como definição por exemplo em [Pillay] e justifica a terminologia e a notação de [Hodges] para o posto interno.

Proposição 2.2.8. RM$(p) \geqslant \xi+1$ se e somente se existem $\mathfrak{B}$ extensão elementar de $\mathfrak{A}$, $X \subseteq Y \subseteq B$ e $q \in S_m^{\mathfrak{B}}(Y)$ com $p \subseteq q$ tal que, para cada $D \in q$ (note que $D \in \mathrm{Def}^m_{\mathfrak{B},Y}$), existem tipos globais distinos $q_i \in \langle D\rangle \subseteq S_m^{\mathfrak{B}}(B)$, $i \in \mathbb{N}$, com RM$(q_i) \geqslant \xi$.

Demonstração: Para a implicação direta, tome $\mathfrak{B}$ ω-saturada, $Y = X$ e $q = p$ como conjuntos de fórmulas. Então RMI$(q) =$ RM$(p) \geqslant \xi + 1$ e aplica-se a proposição anterior para $\mathfrak{B}$, em que RM$(q_i) =$ RMI$(q_i) \geqslant \xi$.

Para a recíproca, fixe $\phi(v) \in p(v)$ arbitrária e assuma a condição no enunciado: ao mostrarmos que RM$(\phi(\mathfrak{A})) \geqslant \xi + 1$, obtemos RM$(p) \geqslant \xi + 1$. Suponha então RM$(\phi(\mathfrak{B})) \leqslant \xi$: como $\phi(\mathfrak{B}) \in q_i$ e RM$(q_i) \geqslant \xi$, obtemos RM$(\phi(\mathfrak{B})) =$ RM$(q_i) = \xi$. Pelas equações de posto, dM$(\phi(\mathfrak{B})) = \sum$ dM(q) com $q \in \langle\phi(\mathfrak{B})\rangle$ e RM$(q) =$ RM$(\phi(\mathfrak{B}))$. Como os tipos q_i são em número infinito, obtemos uma contradição com dM$(\phi(\mathfrak{B})) < \omega$. QED

Desse modo, considerando-se tipos globais, RM$(p) \geqslant \xi + 1$ se e somente se existe uma extensão q de p que é ponto de acumulação, no novo espaço de tipos globais, de tipos de posto $\geqslant \xi$.

O grau de um tipo p com RM$(p) < \infty$ foi definido por Morley como o mínimo limitante do número de extensões de p a Y arbitrário com posto RM(p). Seu artigo mostra que esse limitante é finito, usando união de cadeia, mas é igual ao dM(p) que definimos, bastando tomar $\mathfrak{B}$ ω-saturada e $Y = B$, situação em que as extensões têm grau 1 (irredutíveis têm grau 1) e aplicam-se as equações de posto. Retomaremos esse raciocínio ao discutir deviação (*forking*).

2.3. Transcendência total e Estabilidade

Vimos que os corpos algebricamente fechados têm posto 1, por serem fortemente minimais, de modo que podemos explorá-los melhor no

Exemplo 2.3.1. Dado K um corpo algebricamente fechado, tomamos L uma extensão elementar $|K|^+$-grande de K, ou seja, L é um modelo monstro. É importante, aqui, que todos os tipos sobre K são realizados em L e que L é ω-saturado, estrutura ideal para calcular-se o posto de Morley.

Um tipo de $S_1(K)$ é sempre da forma $t(a/K)$ para $a \in L$.

Se a é algébrico sobre K, então podemos considerar o conjunto D das raízes do polinômio minimal de a sobre K. Temos D finito, definível e com posto 0. Então $t(a/K)$ tem posto 0.

Como K tem posto 1, pelas equações de posto há um tipo com posto 1. Trata-se, portanto, do tipo dos elementos transcendentes sobre K.

Esse exemplo inspirou Morley para a terminologia "totalmente transcendental", que agora exporemos.

Lembramos que A é o máximo da álgebra $\mathrm{Def}^1_{\mathfrak{A},A}$, sendo $\emptyset$-definível pela fórmula $v = v$. Essa mesma fórmula define o domínio B de qualquer estrutura $\mathfrak{B}$, de modo que $\mathrm{RM}_{\mathfrak{A}}(A) = \sup_{\mathfrak{A}\prec\mathfrak{B}} \mathrm{RMI}_{\mathfrak{B}}(B)$.

Se $\mathfrak{A} \equiv \mathfrak{B}$, aplique o Lema 2.1.18 a respectivas extensões elementares ω-saturadas, para obter $\mathrm{RM}_{\mathfrak{A}}(A) = \mathrm{RM}_{\mathfrak{B}}(B)$.

Definição 2.3.2 (Morley). (i) Uma estrutura $\mathfrak{A}$ é *totalmente transcendental* se $\mathrm{RM}_{\mathfrak{A}}(A) < \infty$.

(ii) Uma teoria completa T é *totalmente transcendental* se todo (ou um, como acima) modelo de T for totalmente transcendental.

Assim, as teorias dos corpos algebricamente fechados de característica especificada ACF_0, ACF_p são totalmente transcendentais.

Se $\mathrm{RM}_{\mathfrak{A}}(A) < \infty$ então todo subconjunto definível de A tem posto ou é vazio. Não precisamos restringir-nos a $\mathrm{Def}^1_{\mathfrak{A},A}$:

Lema 2.3.3. Se $\mathrm{RM}_{\mathfrak{A}}(A) = \xi$ então qualquer $D \in \mathrm{Def}^m_{\mathfrak{A},A}$ satisfaz $\mathrm{RM}_{\mathfrak{A}}(D) \leqslant (\xi + 1)^m$, em que esta potência é obtida por produto ordinal.

Referência: O Lema 5.6.9 de [Hodges].

Corolário 2.3.4. Em uma estrutura (ou teoria) totalmente transcendental, todo subconjunto definível não-vazio, e portanto todo tipo, tem posto e grau de Morley.

Para fins de "posto $< \infty$", observamos que não importa qual posto calculemos:

Lema 2.3.5. Uma teoria completa T é totalmente transcendental se e somente se $\mathrm{RMI}_{\mathfrak{A}}(A) < \infty$ para todo modelo $\mathfrak{A}$ de T.

Demonstração: Primeiramente, note que $\mathrm{RM}_{\mathfrak{A}}(A)$ é um supremo de postos, dentre os quais $\mathrm{RMI}_{\mathfrak{A}}(A)$; este é portanto menor ou igual. Se $\mathrm{RMI}_{\mathfrak{B}}(B) < \infty$ para todo modelo $\mathfrak{B}$, em particular para uma extensão elementar ω-saturada $\mathfrak{B}$ de $\mathfrak{A}$, então $\mathrm{RM}_{\mathfrak{A}}(A) = \mathrm{RMI}_{\mathfrak{B}}(B) < \infty$. QED

A terminologia "estabilidade" advém das condições para classificação dos modelos de uma teoria. De algum modo, se esses modelos são classificáveis, devem ser em pouco número; "instável" associa-se, portanto, à realização por muitos modelos. Porém, o leitor notará um melhor uso dessa terminologia na parte (ii) desta definição.

Sejam, por toda a seção, T uma teoria completa com modelos infinitos na linguagem L e κ um cardinal infinito. Diferentemente da Seção 1.4, estas desigualdades ***não*** são estritas e κ-estabilidade ***não*** implica μ-estabilidade para $\mu < \kappa$:

Definição 2.3.6. (i) T é *estável* se ***não*** existem um modelo $\mathfrak{A}$ de T, uma fórmula $\phi(u, v)$ de L, em que u, v são seqüências de r, s variáveis respectivamente, e $a_n \in A^r$, $b_n \in A^s$, $n \in \mathbb{N}$, tais que $\mathfrak{A} \models \phi(a_m, b_n) \Leftrightarrow m \leqslant n$. Caso contrário, T é chamada *instável*.

(ii) T é *κ-estável* se $|S_1^{\mathfrak{A}}(X)| \leqslant \kappa$ para todo modelo $\mathfrak{A}$ de T e todo $X \subseteq A$ com $|X| \leqslant \kappa$. Caso contrário, T é chamada *κ-instável*.

(iii) T é *super-estável* se existe um cardinal infinito μ tal que T é κ-estável para todo $\kappa \geqslant \mu$.

Para uma L-estrutura $\mathfrak{A}$, essas definições referem-se a $Th(\mathfrak{A})$.

Exemplo 2.3.7. Com a linguagem de ordem, $\mathbb{Q}$ não é ω-estável, porque calculamos $|S_1^{\mathbb{Q}}(\mathbb{Q})| = 2^\omega$ no Exemplo 1.3.13. Sua própria ordem mostra que $\mathbb{Q}$ também não é estável.

Exemplo 2.3.8. Na linguagem dos anéis com unidade, as teorias completas que contêm ACF são ω-estáveis. Para tanto, sejam L um corpo algebricamente fechado, $X \subseteq L$ e K o subcorpo gerado por X. Ao longo da Seção 1.3, identificamos $S_1(X) = S_1(K)$ e calculamos $|S_1(K)| = |K| + \omega$. Basta então calcular que $|K| \leqslant |X| \times \omega$, porque os elementos de K são quocientes de elementos obtidos de X por termos, para obter $|S_1(X)| \leqslant \max\{|X|, \omega\}$.

Manipulação adequada das variáveis na definição de estabilidade permite caracterizar essa condição de uitos modos sutilmente distintos: por exemplo, *textbfn ão* existirem um modelo $\mathfrak{A}$ de T, uma fórmula $\psi(x, y)$ de L, em que x, y são seqüências de k variáveis, e $c_i \in A^k$, $i \in \mathbb{N}$, tais que $\mathfrak{A} \models \psi(c_i, c_j) \Leftrightarrow i < j$. Incluir parâmetros nas r-, s- ou k-uplas mostra que, tanto na definição como nesta caracterização, as fórmulas em questão não existem nem em L(A); em particular, se $\mathfrak{A}$ é estável e $X \subseteq A$, também $(\mathfrak{A}, (x)_{x \in X})$ é estável. O Teorema da Compacidade permite ainda substituir a indexação por $\mathbb{N}$ por seqüências finitas arbitrariamente longas ou ordenadas por $\mathbb{Q}$.

Exemplo 2.3.9. Todo domínio de integridade estável é um corpo. Em uma tal estrutura, a relação de divisão é definível por $x|y : x \neq 0 \wedge y \neq 0 \wedge \exists z\,(y = xz)$.

Dado um elemento $a \neq 0$, temos $a^i|a^j$ quando $i \leqslant j$; por estabilidade, existem $i > j$ tais que $a^i|a^j$. Como também $a^j|a^{i-1}$, conclui-se que $a|1$.

Uma primeira observação é que, novamente, não precisamos restringir-nos a 1-tipos:

Lema 2.3.10. Se T é κ-estável, então $|S_m^{\mathfrak{A}}(X)| \leqslant \kappa$ para todos $m \in \mathbb{N}^*$, modelo $\mathfrak{A}$ de T e $X \subseteq A$ com $|X| \leqslant \kappa$.

Referências: O Lema 6.7.4 de [Hodges] ou o Corolário I, 2.2 de [Shelah].

Evidentemente, devemos relacionar estabilidade e κ-estabilidade, cujas definições são distintas. Este é um teorema central da Estabilidade, porém de uma longa demonstração sem relação com nosso material:

Teorema 2.3.11. T é estável se e somente se existe um cardinal infinito κ para o qual T é κ-estável.

Referências: O Teorema 6.7.2 de [Hodges] ou o Teorema 2.10 e a Conclusão 2.11 do Capítulo I de [Shelah].

Esta é a movimentada via da estabilidade, sendo a equivalência de transcendência total e ω-estabilidade devida a Morley quando $|\mathrm{L}| = \omega$.

Teorema 2.3.12. Se T é totalmente transcendental, então T é super-estável; mais precisamente, T é κ-estável para todo $\kappa \geqslant |\mathrm{L}|$. Reciprocamente, se T é ω-estável, então T é totalmente transcendental.

Demonstração: Se T é totalmente transcendental, $\mathfrak{A} \models T$ e $X \subseteq A$, então todo tipo sobre X tem posto e determina um X-definível, ou seja, uma fórmula de $\mathrm{L}(X)$. Pelo Lema 2.2.3, $|S_1(X)| \leqslant |\mathrm{L}(X)| = |\mathrm{L}| + |X|$.

Se T não é totalmente transcendental, existe $\mathfrak{A} \models T$ com $\mathrm{RMI}_{\mathfrak{A}}(A) = \infty$ pelo Lema 2.3.5. Já o Lema 2.1.8 mostra a existência de uma árvore binária de definíveis sem posto $A_s \neq \emptyset$, s seqüência finita sobre $\{0,1\}$, de modo que $A_\emptyset = A$, $A_{s0}, A_{s1} \subseteq A_s$ e $A_{s0} \cap A_{s1} = \emptyset$. Como a árvore é enumerável, podemos tomar enumerável o conjunto X dos parâmetros necessários para definir todos os A_s.

Cada ramo da árvore, dado por $\sigma \in \{0,1\}^{\mathbb{N}}$, tem a propriedade da intersecção finita e estende-se a um tipo $p_\sigma \in S_1(X)$. Os tipos p_σ são todos distintos, pois onde um ramo bifurca há dois definíveis disjuntos, e são portanto em quantidade 2^ω, de modo que $S_1(X)$ não é enumerável. QED

Apenas mencionamos os Exercícios 6 e 7 da Seção 6.7 de [Hodges]: (i) Tome L a linguagem com predicados unários P_n, $n \in \mathbb{N}$, e tome $\mathfrak{A} = (\mathbb{N}^*, (R_n)_{n\in\mathbb{N}})$

com R_n o conjunto dos números divisíveis pelo n-ésimo primo. Então $\mathfrak{A}$ é super-estável, mas não totalmente transcendental. (ii) Tome L a linguagem com predicados binários P_n, $n \in \mathbb{N}$, e tome T a teoria das sentenças que expressam "P_n é uma relação de equivalência" e "cada classe de P_n é união de infinitas classes de P_{n+1}". Então T é estável mas não super-estável.

Há outras caracterizações dos conceitos que definimos nesta seção, das quais procuramos exibir algumas de maior freqüência. O leitor também pode consultar [Pillay], em especial sua Seção 1.4, ou [Poizat 1].

Introduziremos futuramente a noção de tipo definível, mas já enunciamos aqui o

Teorema 2.3.13. Equivalem: T é estável; todos os tipos (não necessariamente globais) sobre modelos de T são definíveis; T é κ-estável para todo κ que satisfaz $\kappa = \kappa^{|L|}$.

Referência: O Teorema 6.7.13 de [Hodges].

Sabe-se também que T é super-estável se e somente se T é estável em todo cardinal $\kappa \geqslant 2^{|L|}$.

Finalmente, este é o mais simples de uma série de teoremas de Estabilidade:

Teorema 2.3.14 (Harnik). Se $\kappa \geqslant |L|$ e T é κ-estável, então tem um modelo saturado de cardinalidade κ.

Referência: O Teorema 14.2 de [Poizat 1].

Ao aplicarmos estes dois teoremas, concluímos que toda teoria estável tem modelos saturados de cardinalidades arbitrariamente grandes.

2.4. Dois teoremas úteis

Provaremos, sob algumas hipóteses, dois teoremas úteis. O primeiro informa que o conjunto dos parâmetros usados para definir conjuntos "grandes", em uma caracterização envolvendo posto de Morley, é ele próprio definível. O segundo mostra que tipos globais com posto ordinal têm grau 1: esta é uma informação potente quando aliada às equações de posto.

Há duas abordagens para esse tema, apresentadas uma em [Hodges] e a outra em [MTAG] e [Marker] — a primeira deve-se a Shelah e a segunda a Lachlan: veja os comentários históricos dessas referências. Em [Hodges], a única condição necessária é estabilidade, como mostra o Teorema 2.3.13; a linha de [MTAG] e [Marker] requer ω-saturação e transcendência total (mais precisamente ω-estabilidade), mas seu raciocínio aproxima-se melhor do uso de que faremos.

Para obter o melhor de cada abordagem, *assumiremos apenas estabilidade e que os tipos necessários tenham posto ordinal.*

Suponha $\mathfrak{A}$ uma L-estrutura estável e $X \subseteq A$. Tome $\mathfrak{B}$ uma extensão elementar ω-saturada de $\mathfrak{A}$ e $\mathfrak{C}$ uma extensão elementar κ-grande de $\mathfrak{B}$, com $\kappa > |\mathrm{L}|, |B|$. Como $\mathfrak{C} \equiv \mathfrak{A}$, também $\mathfrak{C}$ é estável. Serão importantes, ainda, o fato de $\mathfrak{C}$ ser $|B|^+$-saturado e a Proposição 1.4.6.

Destacamos dois lemas técnicos:

Lema 2.4.1. Suponha w uma seqüência de n variáveis livres e $\phi_i(w), \psi_j(w)$ fórmulas de $\mathrm{L}(C)$ para $i \in I$, $j \in J$, de modo que $|I|, |J| < \kappa$ e $\bigcup_{i\in I} \phi_i(\mathfrak{C}) = C^n - \bigcup_{j\in J} \psi_j(\mathfrak{C})$. Então existe um subconjunto finito I_0 de I tal que $\bigcup_{i\in I} \phi_i(\mathfrak{C}) = \bigcup_{i\in I_0} \phi_i(\mathfrak{C})$.

Demonstração: Este é o Exercício 4.5.34 de [Marker]. É esclarecedor reescrever o enunciado usando "disjunções infinitas". Afirma-se que, se $\bigvee_{i\in I} \phi_i$ equivale a $\neg\big(\bigvee_{j\in J} \psi_j\big)$ em $\mathfrak{C}$, então equivale também a uma disjunção finita $\bigvee_{i\in I_0} \phi_i$.

Seja Y o conjunto de todos os parâmetros de C nas fórmulas ϕ_i, ψ_j. Como estas são finitas, temos $|Y| \leqslant |I| \times \omega + |J| \times \omega < \kappa$. Então todos os tipos sobre Y são principais. Mas, se $c \in C^n$ e $\theta(w)$ é uma fórmula qualquer de $\mathrm{L}(Y)$, vale

$$t(c/Y) \in \langle \theta(\mathfrak{C}) \rangle \Leftrightarrow \theta(\mathfrak{C}) \in t(c/Y) \Leftrightarrow c \in \theta(\mathfrak{C}) .$$

Desse modo, $\bigcup_{i\in I} \langle \phi_i(\mathfrak{C}) \rangle = S_n(Y) - \bigcup_{j\in J} \langle \psi_j(\mathfrak{C}) \rangle$.

Sendo o membro direito dessa igualdade um fechado em $S_n(Y)$ compacto, vemos que existe I_0 subconjunto finito de I tal que $\bigcup_{i\in I_0} \langle \phi_i(\mathfrak{C}) \rangle = \bigcup_{i\in I} \langle \phi_i(\mathfrak{C}) \rangle$. Novamente, temos $\bigcup_{i\in I_0} \phi_i(\mathfrak{C}) = \bigcup_{i\in I} \phi_i(\mathfrak{C})$. QED

Lema 2.4.2. Sejam v uma seqüência de m variáveis, $\theta(v)$ fórmula de $\mathrm{L}(B)$ e $\pi(v)$ fórmula de $\mathrm{L}(C)$. Suponha que $\mathrm{RM}(\theta(\mathfrak{C})) = \mathrm{RM}((\theta \wedge \pi)(\mathfrak{C})) = \xi$. Então existe $b \in B^m$ tal que $\mathfrak{C} \models (\theta \wedge \pi)(b)$.

Demonstração: Trata-se de mostrar que, de certo modo, $\theta(\mathfrak{B})$ já é suficientemente grande. Note que, por outro lado, não faz sentido considerar $\pi(\mathfrak{B})$, já que B pode não conter os parâmetros de π.

Procedemos por indução em ξ. Se $\xi = 0$, então $\theta(\mathfrak{C})$ é finito e $\mathfrak{B} \models \exists^{=|\theta(\mathfrak{C})|} v\, \theta(v)$, donde $|\theta(\mathfrak{B})| = |\theta(\mathfrak{C})|$ finito e obtemos $\theta(\mathfrak{B}) = \theta(\mathfrak{C})$; porém $(\theta \wedge \pi)(\mathfrak{C}) \neq \emptyset$ porque tem posto ξ.

Se $\xi > 0$ e $\mathrm{dM}(\theta(\mathfrak{C})) = n > 1$, como $\mathfrak{C}$ é ω-saturada particionamos $\theta(\mathfrak{C}) = D_1 \cup \ldots \cup D_n$ com D_i definíveis também de posto ξ. Então algum $D_i \cap \pi(\mathfrak{C})$ tem posto ξ; caso contrário a união teria posto $< \xi$. Podemos assim supor $n = 1$.

Nesse caso, $(\theta \wedge \neg\pi)(\mathfrak{C})$ tem posto $R < \xi$, por sua união com $(\theta \wedge \pi)(\mathfrak{C})$ ser $\theta(\mathfrak{C})$. Se $R = -1$ então $\theta(\mathfrak{C}) \subseteq \pi(\mathfrak{C})$ e basta tomar qualquer $b \in \theta(\mathfrak{B})$. Para $R \geqslant 0$, como $\mathfrak{B}$ é ω-saturada, podemos usar o Lema 2.1.10 com o posto geral. Observe que $\mathrm{RM}(\theta(\mathfrak{B})) = \xi$: existem então fórmulas $\theta_n(v)$, $n \in \mathbb{N}$, de $\mathrm{L}(B)$ de modo que $\theta_n(\mathfrak{B})$ são dois a dois disjuntos contidos em $\theta(\mathfrak{B})$ com posto R, valendo o mesmo para $\theta_n(\mathfrak{C})$ em $\theta(\mathfrak{C})$. Para algum n, $(\theta_n \wedge \neg\pi)(\mathfrak{C}) = \theta_n(\mathfrak{C}) \cap (\theta \wedge \neg\pi)(\mathfrak{C})$ tem posto $< R$: de fato, para todos exceto um número finito. Vem $\mathrm{RM}((\theta_n \wedge \pi)(\mathfrak{C})) = R$ e então existe $b \in B^m$ com $b \in (\theta_n \wedge \pi)(\mathfrak{C})$. Assim, $\mathfrak{C} \models \theta(b), \pi(b)$ como desejado. QED

Teorema 2.4.3. Sejam $D \in \mathrm{Def}^m_{\mathfrak{C},X}$ com posto ξ e $\phi(v,w)$ fórmula de L com v, w seqüências de m, n variáveis respectivamente. Então $\{c \in C^n | D \subseteq_\xi \phi(\mathfrak{C}, c)\}$ é X-definível em $\mathfrak{C}$.

Demonstração: Mostraremos que esse conjunto Γ é definível. Contudo, Γ é invariante sob os automorfismos sobre X, porque se σ é um tal automorfismo e $c \in \Gamma$ então $D = \sigma[D] \subseteq_\xi \phi(\mathfrak{C}, \sigma(c))$ e $\sigma(c) \in \Gamma$, sendo a recíproca analogamente verdadeira. Como $\kappa > |X|$, o conjunto Γ é X-definível pela Proposição 1.4.6.

Reduzimos ao caso em que D tem grau 1. Escreva $d = \mathrm{dM}(D)$ e particione $D = D_1 \cup \ldots \cup D_d$ definíveis de posto ξ e grau 1. Então $D \subseteq_\xi E \Leftrightarrow D_1 \subseteq_\xi E$ e $\ldots$ e $D_d \subseteq_\xi E$, já que $D - E = (D_1 - E) \cup \ldots \cup (D_d - E)$. Assim,

$$\{c \in C^n \mid D \subseteq_\xi \phi(\mathfrak{C}, c)\} = \bigcap_{i=1}^{d} \{c \in C^n \mid D_i \subseteq_\xi \phi(\mathfrak{C}, c)\} .$$

Assuma então $\mathrm{dM}(D) = 1$. Podemos também supor $\{c \in C^n \mid D \subseteq_\xi \phi(\mathfrak{C}, c)\}$ não-vazio. Seja $D(\mathfrak{B})$ o conjunto definido em $\mathfrak{B}$ pela fórmula de $\mathrm{L}(X)$ que define D em $\mathfrak{C}$.

Suponha $c \in C^n$ com $D \subseteq_\xi \phi(\mathfrak{C}, c)$. Mostraremos, primeiramente, que $D(\mathfrak{B})$ contém um subconjunto finito D_0 tal que $D_0 \subseteq \phi(\mathfrak{C}, c)$ e, para todo $b \in C^n$, valha a implicação

$$D_0 \subseteq \phi(\mathfrak{C}, b) \Rightarrow D \subseteq_\xi \phi(\mathfrak{C}, b) .$$

Se D_0 não existe, construímos $a_i \in C^m$, $b_i \in C^n$, $i \in \mathbb{N}$, assim: suponha $a_0, \ldots, a_{k-1}, b_0, \ldots, b_{k-1}$ construídos para $k \geqslant 0$ de modo que $a_i \in D(\mathfrak{B}) \cap \phi(\mathfrak{C}, c)$ e $D \not\subseteq_\xi \phi(\mathfrak{C}, b_i)$. Temos $\mathrm{RM}(D \cap \phi(\mathfrak{C}, c)) = \xi$ e, por D ser irredutível, $\mathrm{RM}(D \cap \phi(\mathfrak{C}, c) \cap \phi(\mathfrak{C}, b_i)) < \xi$. Concluímos que $\mathrm{RM}((D \cap \phi(\mathfrak{C}, c)) - (\phi(\mathfrak{C}, b_0) \cup \ldots \cup \phi(\mathfrak{C}, b_{k-1})) = \xi$ e, pelo segundo lema, existe $a_k \in D(\mathfrak{B}) \cap (\phi(\mathfrak{C}, c) - \bigcup_{i=0}^{k-1} \phi(\mathfrak{C}, b_i))$. Mas $\{a_0, \ldots, a_{k-1}\}$, por ser finito, não tem a propriedade desejada para D_0 (que supomos não existir). Então existe $b_k \in C^n$ tal que

$\{a_0, \ldots, a_{k-1}, a_k\} \subseteq \phi(\mathfrak{C}, b_k)$ e $D \not\subseteq_\xi \phi(\mathfrak{C}, b_k)$. Por construção, $a_k \notin \phi(\mathfrak{C}, b_j)$ para $j < k$. Assim,

$$\mathfrak{C} \models \phi(a_i, b_j) \Leftrightarrow a_i \in \phi(\mathfrak{C}, b_j) \Leftrightarrow i \leqslant j\ ,$$

contradizendo a estabilidade de $\mathfrak{C}$.

Seja $\mathscr{D}$ o conjunto dos subconjuntos finitos D_0 de $D(\mathfrak{B})$ assim obtidos, um para cada $c \in C^n$ com $D \subseteq_\xi \phi(\mathfrak{C}, c)$. Para $D_0 \in \mathscr{D}$, seja $\chi_{D_0}(w)$ a fórmula de $L(C)$ que expressa "$D_0 \subseteq \phi(\mathfrak{C})(w)$" — existe porque D_0 é finito. Para qualquer $c \in C^n$, obtemos: $D \subseteq_\xi \phi(\mathfrak{C}, c)$ se e somente se existe $D_0 \in \mathscr{D}$ com $\mathfrak{C} \models \chi_{D_0}(c)$. Temos também $|\mathscr{D}| \leqslant |D(\mathfrak{B})|\omega \leqslant |B|^m\omega < \kappa$.

Com o mesmo raciocínio aplicado a $\neg\phi$, obtemos fórmulas ψ_j, $j \in J$ com $|J| < \kappa$, tais que $D \subseteq_\xi (\neg\phi)(\mathfrak{C}, c)$ se e somente se existe $j \in J$ tal que $\mathfrak{C} \models \psi_j(c)$.

Novamente, $D \subseteq_\xi \phi(\mathfrak{C}, c) \Leftrightarrow D \not\subseteq_\xi (\neg\phi)(\mathfrak{C}, c)$ e obtemos precisamente as condições do primeiro lema: existem $D_1, \ldots, D_k \in \mathscr{D}$ tais que $D \subseteq_\xi \phi(\mathfrak{C}, c)$ se e somente se $\mathfrak{C} \models \chi_{D_1}(c) \vee \ldots \vee \chi_{D_k}(c)$. QED

Para este resultado, adaptamos os raciocínios da pág. 232 e do Corolário 6.3.12 de [Marker]:

Teorema 2.4.4 (Lachlan). Todo tipo global com posto (ordinal) tem grau 1.

Demonstração: Suponha $p \in S_m^{\mathfrak{B}}(A)$ e $q \in S_m^{\mathfrak{B}}(B)$ com $p \subseteq q$ e $\mathrm{RM}(p) = \mathrm{RM}(q) = \xi$; temos $\mathrm{dM}(q) = 1$ porque $\mathfrak{B}$ é ω-saturada e q é global em $\mathfrak{B}$. Devemos mostrar que também $\mathrm{dM}(p) = 1$. Sejam $D \in p$ determinado por p tendo posto ξ e grau $\mathrm{dM}(p)$ e $E \in q$ determinado por q tendo posto ξ e grau 1. Note que $D \cap E \in q$ ainda tem posto ξ e grau 1 por minimalidade: podemos então supor $E \subseteq D$. Escreva $D = \phi(\mathfrak{B})$ e $E = \psi(\mathfrak{B}, b)$, com $\phi(v)$ fórmula de $L(A)$ e $\psi(v, w)$ fórmula de L, v, w seqüências de m, n variáveis respectivamente e $b \in B^n$, de modo que $\mathfrak{B} \models \forall v\,(\psi(v, b) \to \phi(v))$.

Tome $S_1 = \{c \in C^n \mid \mathfrak{C} \models \forall v\,(\psi(v, c) \to \phi(v))\}$ $\{c \in C^n \mid \phi(\mathfrak{C}) \subseteq_\xi (\neg\psi)(\mathfrak{C}, c)\}$. O primeiro conjunto é A-definível, assim como o segundo pelo teorema anterior (com $X = A$), já que $\mathrm{RM}(\phi(\mathfrak{C})) = \xi$. Então $S_1 = \{c \in C^n \mid \psi(\mathfrak{C}, c) \subseteq \phi(\mathfrak{C})$ e tem posto $\xi\}$ é A-definível. Analogamente, $S_2 = \{(c, d) \in C^{n+n} \mid \psi(\mathfrak{C}, c) \cap \psi(\mathfrak{C}, d) \subseteq \phi(\mathfrak{C})$ e tem posto $\xi\}$ e $S_3 = \{(c, d) \in C^{n+n} \mid \psi(\mathfrak{C}, c) \cap (\neg\psi)(\mathfrak{C}, d) \subseteq \phi(\mathfrak{C})$ e tem posto $\xi\}$ são A-definíveis. Obtemos o A-definível $S = \{c \in C^n \mid c \in S_1$ e $(c, d) \notin S_2 \cap S_3$ para todo $d \in C^n\}$, que é o conjunto dos $c \in C^n$ tais que $\psi(\mathfrak{C}, c) \subseteq \phi(\mathfrak{C})$, $\psi(\mathfrak{C}, c)$ tem posto ξ e, para todo $d \in C^n$, $\mathrm{RM}(\psi(\mathfrak{C}, c) \cap \psi(\mathfrak{C}, d)) < \xi$ ou $\mathrm{RM}(\psi(\mathfrak{C}, c) - \psi(\mathfrak{C}, d)) < \xi$. Note que $b \in S$ porque $\psi(\mathfrak{C}, b)$ tem grau 1.

Tome $R = S_2 \cap (S \times S) = \{(c,d) \in S \times S \mid \mathrm{RM}(\psi(\mathfrak{C},c) \cap \psi(\mathfrak{C},d)) = \xi\}$, A-definível. Mostremos que R é uma relação de equivalência em S com número finito de classes, observando que $(b,b) \in R$. Evidentemente, R é simétrica e reflexiva. Suponha $(c,d),(d,e) \in R$. Então $\psi(\mathfrak{C},d) \cap \psi(\mathfrak{C},e)$ tem posto ξ e está contido em

$$(\psi(\mathfrak{C},d) - \psi(\mathfrak{C},c)) \cup (\psi(\mathfrak{C},c) \cap \psi(\mathfrak{C},e))\,,$$

que portanto tem posto $\geqslant \xi$. Também $\psi(\mathfrak{C},d) \cap \psi(\mathfrak{C},c)$ tem posto ξ: pela caracterização de S, então $\psi(\mathfrak{C},d) - \psi(\mathfrak{C},c)$ tem posto $< \xi$. Concluímos que $\psi(\mathfrak{C},c) \cap \psi(\mathfrak{C},e)$ tem posto ξ e $(c,d) \in R$. Agora, suponha $c_1,\ldots,c_k \in S$ representantes de classes distintas de R. Temos $\psi(\mathfrak{C},c_i) \subseteq \phi(\mathfrak{C})$, mas $\mathrm{RM}(\psi(\mathfrak{C},c_i)) = \xi$ e $\mathrm{RM}(\psi(\mathfrak{C},c_i) \cap \psi(\mathfrak{C},c_j)) < \xi$ para $i \neq j$, donde $k \leqslant \mathrm{dM}(\phi(\mathfrak{C})) = \mathrm{dM}(p)$.

Como S e R são A-definíveis e R tem um número *finito* de classe de equivalência — fatos todos descritos por fórmulas de $\mathrm{L}(A)$ —, todas as classes de R intersectam A^n.

Tome $a \in A^n$ na mesma classe de b. Então $\psi(\mathfrak{C},a) \subseteq \phi(\mathfrak{C})$ tem posto ξ, $\psi(\mathfrak{C},a) \cap \psi(\mathfrak{C},b)$ tem posto ξ, mas $\psi(\mathfrak{C},a) - \psi(\mathfrak{C},b)$ tem posto $< \xi$. Já que $\psi(\mathfrak{C},b)$ tem grau 1, concluímos que $\psi(\mathfrak{C},a)$ tem grau 1.

Finalmente, temos $\psi(\mathfrak{B},a)$ de posto ξ e grau 1 (lembre que ψ é fórmula de L e $a \in A^n$) contido em $\phi(\mathfrak{B})$. Se $\mathrm{RM}(\phi(\mathfrak{B}) - \psi(\mathfrak{B},a)) < \xi$, então $\mathrm{dM}(p) = \mathrm{dM}(\phi(\mathfrak{B})) = 1$. Caso contrário, $\mathrm{dM}(\phi(\mathfrak{B}) - \psi(\mathfrak{B},a)) < \mathrm{dM}(\phi(\mathfrak{B}))$, de modo que $\phi(\mathfrak{B}) - \psi(\mathfrak{B},a) \notin p$ e obtemos $\psi(\mathfrak{B},a) \in p$ e $\mathrm{dM}(p) = 1$. QED

Assim, se $D \in \mathrm{Def}_A^m$ é um irredutível, D determina um tipo global e tem $\mathrm{dM}(D) = 1$.

2.5. Deviação (*forking*) e independência

Este é um tópico importante sobre o qual, contudo, seremos breves por falta de espaço. Sua existência e teoria devem-se a Shelah; um tratamento alternativo é chamado "parisiense", baseado em uma "ordem fundamental" e exposto em [Poizat 1] e no livro de Lascar que mencionamos na introdução do capítulo. Fundamentamos nossa apresentação no que, nas outras abordagens, é apenas uma caracterização: a conservação do posto de Morley.

Assumiremos que todos os tipos com que trabalharmos têm posto (ordinal). Fixe uma estrutura $\mathfrak{A}$ e, inicialmente, suponha $X \subseteq Y \subseteq A$.

Sejam $p \in S_m(X)$, $q \in S_m(Y)$. Sabemos que, por definição, se $p \subseteq q$ então $\mathrm{RM}(q) \leqslant \mathrm{RM}(p)$. Estudaremos a situação em que ocorre igualdade:

Definição 2.5.1. (i) q é uma extensão *direta* de p se contém p e tem o mesmo posto que p. (Diz-se *nonforking* em inglês.)

(ii) Se q é uma extensão direta de $q|_X$, dizemos que q ***não** se desvia* sobre X. (Diz-se *not forks* em inglês.)

Proposição 2.5.2 (Existência). As extensões q sobre Y indivisíveis de um tipo p sobre X satisfazem $\sum \mathrm{dM}(q) = \mathrm{dM}(p)$. Em particular: p tem entre uma e $\mathrm{dM}(p)$ extensões indivisíveis; esse máximo é alcançado se $Y = A$; se houver uma extensão com grau $\mathrm{dM}(p)$, será a única extensão.

Demonstração: Sendo $D \in \mathrm{Def}_X^m$ determinado por p, mostraremos que as extensões indivisíveis de p em $S_m(Y)$ são precisamente os tipos $q \in \langle D \rangle$ com $\mathrm{RM}(q) = \mathrm{RM}(D)$. Feito isso, aplicamos o Corolário 2.2.5 em $S_m(Y)$: $\mathrm{dM}(p) = \mathrm{dM}(D) = \sum \mathrm{dM}(q)$ com $q \in \langle D \rangle$ e $\mathrm{RM}(q) = \mathrm{RM}(D)$.

Se q é uma extensão direta de p, então $\mathrm{RM}(q) = \mathrm{RM}(p) = \mathrm{RM}(D)$ e $D \in q$. Por outro lado, suponha que $D \in q$ e $\mathrm{RM}(q) = \mathrm{RM}(D) = \mathrm{RM}(p)$. Então $\mathrm{RM}(q|_X) \geqslant \mathrm{RM}(q) = \mathrm{RM}(D)$, mas $D \in q|_X$, de modo que $\mathrm{RM}(q|_X) = \mathrm{RM}(D)$. Suponha que $q|_X$ determine E. Então $D \cap E \in q|_X$ e, por minimalidade, $\mathrm{RM}(D \cap E) = \mathrm{RM}(q|_X)$ e $\mathrm{dM}(D \cap E) = \mathrm{dM}(q|_X)$, ou seja, $q|_X$ determina $D \cap E$. Mas $\mathrm{dM}(D \cap E) \leqslant \mathrm{dM}(D)$; por D ser irredutível em Def_X^m, temos $\mathrm{dM}(q|_X) = \mathrm{dM}(D)$ e D determina $q|_X$. Pela Proposição 2.2.4, temos $p = q|_X$, donde $p \subseteq q$ e q é uma extensão direta de p. QED

Desse modo, um tipo global (com posto e sobre uma estrutura estável) tem uma única extensão direta.

Estas propriedades serão repetidamente utilizadas:

Fato 2.5.3 (Transitividade e Monotonicidade). Sejam $p \subseteq q \subseteq r$ tipos. Então r é uma extensão direta de p se e somente se r é uma extensão direta de q e q é uma extensão direta de p.

Pois $p \subseteq q \subseteq r$ implica $\mathrm{RM}(p) \geqslant \mathrm{RM}(q) \geqslant \mathrm{RM}(r)$.

Exemplo 2.5.4 (Continuidade). Seja $D \in q$ determinado por esse tipo. Tome Y_0 um subconjunto finito de Y de modo que D seja Y_0-definível. Então $D \in q|_{Y_0}$, donde $\mathrm{RM}(q|_{Y_0}) = \mathrm{RM}(q)$ e $\mathrm{dM}(q|_{Y_0}) = \mathrm{dM}(q)$. Basta então invocar a unicidade, no caso particular da Proposição de Existência, para concluir que q é a única extensão direta de $q|_{Y_0}$ a Y. Assuma agora que q desvia-se sobre X. Também $D \in q|_{Y_0X}$, donde $\mathrm{RM}(q|_{Y_0X}) = \mathrm{RM}(q) > \mathrm{RM}(q|_X)$ e concluímos que $q|_{X\cup Y_0}$ ainda se desvia sobre X.

Introduziremos o conceito de independência, primeiramente de m-uplas e depois de conjuntos. Veremos uma caracterização geométrica na Seção 3.4.

Suponha agora $X, Y, U, W \subseteq A$ e $x = (x_1, \ldots, x_m) \in A^m$, $m \neq 0$.

Definição 2.5.5. Dizemos que x *independe de U sobre X* e indicamos $x \mathop{\smile\!\!\!\!\!\!|}_X U$ se $t(x/XU)$ não se desvia sobre X, ou seja, $t(x/XU)$ é extensão direta de $t(x/XU)|_X = t(x/X)$. Usaremos o símbolo $\not\mathop{\smile\!\!\!\!\!\!|}$ para negar essa relação.

Observamos que, na notação $x \mathop{\smile\!\!\!\!\!\!|}_X y$, trata-se x como uma seqüência de elementos e y como um conjunto, notadamente o dos elementos que ocorrem na seqüência y.

Novamente, destacamos estas propriedades de uso repetido:

Corolário 2.5.6 (Transitividade e Monotonicidade). $x \mathop{\smile\!\!\!\!\!\!|}_{XY} U$ e $x \mathop{\smile\!\!\!\!\!\!|}_X Y$ se e somente se $x \mathop{\smile\!\!\!\!\!\!|}_X YU$.

Note que $t(x/X) \subseteq t(x/XY) \subseteq t(x/XYU)$, aplicando-se o fato homônimo.

Proposição 2.5.7 (Base finita). $x \mathop{\smile\!\!\!\!\!\!|}_X U$ se e somente se $x \mathop{\smile\!\!\!\!\!\!|}_X U_0$ para todo subconjunto finito U_0 de U, ou seja, $x \mathop{\smile\!\!\!\!\!\!|}_X y$ para toda seqüência y (não-vazia) de elementos de U.

Demonstração: Temos $\mathrm{RM}(x/X) \leqslant \mathrm{RM}(x/XU_0) \leqslant \mathrm{RM}(x/XU)$ para cada U_0, o que prova a implicação direta. Para a recíproca, suponha que x não independa de U sobre X, existindo $D \in t(x/XU)$ com $\mathrm{RM}(D) < \mathrm{RM}(x/X)$. Como a fórmula que define D tem um número finito de parâmetros, existe U_0 subconjunto finito de U tal que D é XU_0-definível. Então x não independe de U_0 sobre X. QED

Este é o resultado de que mais faremos uso:

Teorema 2.5.8 (Simetria). Sejam $x \in A^m$, $y \in A^n$ com $m, n \neq 0$. Se $x \mathop{\smile\!\!\!\!\!\!|}_X y$ então $y \mathop{\smile\!\!\!\!\!\!|}_X x$ (valendo a recíproca por simetria).

Demonstração: Como já fizemos anteriormente, consideraremos a cadeia $\mathfrak{A} \prec \mathfrak{B} \prec \mathfrak{C}$ em que $\mathfrak{B}$ é ω-saturada e $\mathfrak{C}$ é $|B|^+$-grande. Trabalharemos diretamente com os tipos e o posto de Morley em $\mathfrak{C}$.

Assuma $\mathrm{RM}(x/Xy) = \mathrm{RM}(x/X)$ para mostrar que $\mathrm{RM}(y/Xx) = \mathrm{RM}(y/X)$. Escreva $\mathrm{RM}(x/X) = \xi$ e $\mathrm{RM}(y/X) = \zeta$.

Tome $y' \in C^n$ realizando uma extensão direta de $t(y/X)$ a B. Então $\mathrm{RM}(y'/B) = \zeta$. Porque $\mathfrak{C}$ é $|B|^+$-saturada e $Xy' < |B|$, também existe $c \in C^m$ tal que $t(x, y/X) = t(c, y'/X)$. Substituir y por y' é uma bijeção definível que nos permite concluir que $\mathrm{RM}(x/Xy) = \mathrm{RM}(c/Xy')$ e $\mathrm{RM}(x/X) = \mathrm{RM}(c/X)$.

Tome $x' \in C^m$ realizando uma extensão direta de $t(c/Xy')$ a By'. Então $\mathrm{RM}(x'/By') = \mathrm{RM}(c/Xy') = \mathrm{RM}(x/Xy) = \xi$. Note que $t(c/X) \subseteq t(x'/B)$, de modo que $\mathrm{RM}(x'/B) \leqslant \mathrm{RM}(c/X) = \mathrm{RM}(x/X) = \xi = \mathrm{RM}(x'/By') \leqslant \mathrm{RM}(x'/B)$, donde $\mathrm{RM}(x'/B) = \xi$. Também $t(x, y/X) = t(x', y'/X)$, de modo que $\zeta = \mathrm{RM}(y/X) \geqslant \mathrm{RM}(y/Xx) - \mathrm{RM}(y'/Xx') \geqslant \mathrm{RM}(y'/Bx')$.

Assim, reduzimos o problema $[x, y, X]$ à situação $[x', y', B]$, em que B é o domínio de uma estrutura ω-saturada e basta mostrar $\mathrm{RM}(y'/Bx') = \zeta$.

Suponha que exista uma fórmula $\theta(v, w)$ de $\mathrm{L}(B)$, com v, w seqüências de m, n variáveis, tal que $\mathfrak{C} \models \theta(x', y')$ e que $\theta(x', \mathfrak{C}) \in t(y'/Bx')$ tenha posto $< \zeta$. Sejam ainda $D \in \mathrm{Def}^m_{\mathfrak{C},B}$ e $E \in \mathrm{Def}^n_{\mathfrak{C},B}$ com $D \in t(x'/B)$ e $E \in t(y'/B)$ determinados por esses tipos, ou seja, $\mathrm{RM}(D) = \xi$ e $\mathrm{RM}(E) = \zeta$.

Pelo Teorema 2.4.3, o conjunto $Z = \{c \in C^m \mid E \subseteq_\zeta (\neg\theta, c, \mathfrak{C})\}$ é B-definível.

Temos $x' \in D \cap \theta(\mathfrak{C}, y') \cap Z$, de modo que este conjunto pertence a $t(x'/By')$ e, portanto, tem posto $\geqslant \xi$. Como está contido em D, concluímos que seu posto é precisamente ξ.

Recorde que D é B-definível e $D \cap \theta(\mathfrak{C}, y') \cap Z$ é C-definível, ambos com posto ξ. Pelo Lema 2.4.2, existe $x'' \in B^m$ tal que $x'' \in D \cap \theta(\mathfrak{C}, y') \cap Z$, ou seja, $\mathfrak{C} \models \theta(x'', y')$ e $E \cap \theta(x'', \mathfrak{C})$ tem posto $< \zeta$, donde $\mathrm{RM}(y'/B) < \zeta$, contradição.

QED

Concluímos com uma generalização:

Definição 2.5.9. Dizemos que U *independe de* V *sobre* X e indicamos $U \perp_X V$ se todas as m-uplas de U, $m \in \mathbb{N}^*$, independem de V sobre X.

Corolário 2.5.10 (Simetria). Se $U \perp_X V$ então $V \perp_X U$.

Demonstração: Seja $y = (y_1, \ldots, y_n) \in V^n$, $n \in \mathbb{N}$, uma seqüência arbitrária de elementos de V. Devemos mostrar que $y \perp_X U$, ou seja, $t(y/XU)$ não se desvia sobre X.

Por continuidade, caso $t(y/XU)$ divida-se sobre X, existe um subconjunto finito U_0 de U tal que $t(y/XU_0) = t(y/XU)|_{XU_0}$ desvia-se sobre X. Tome x uma $|U_0|$-upla de U formada pelos elementos de U_0 sem repetição. Assim, $t(y/Xx)$ desvia-se sobre X.

Por hipótese, $x \perp_X V$ e $t(x/XV)$ é extensão direta de $t(x/X)$. Mas $t(x/X) \subseteq t(x/Xy) \subseteq t(x/XV)$, donde $t(x/Xy)$ é extensão direta de $t(x/X)$, ou seja, $x \perp_X y$. Por simetria, $y \perp_X x$, ou seja, $t(y/Xx)$ é extensão direta de $t(y/X)$, contradição. QED

Corolário 2.5.11 (Transitividade e Monotonicidade). Valem $V \perp_{XY} U$ e $V \perp_X Y$ se e somente se $V \perp_X YU$.

Basta aplicar o corolário homônimo a cada seqüência de elementos de V.

2.6. Tipos definíveis e herdeiros

Esta seção provê uma caracterização sintática da extensão direta de um posto global, sob as hipóteses de estabilidade e tipo com posto ordinal. Contudo, alguns dos resultados apresentados são válidos em quaisquer condições.

Esta definição esclarece o enunciado do Teorema 2.3.13:

Definição 2.6.1. Suponha $\mathfrak{A}$ uma L-estrutura arbitrária e $X, Y \subseteq A$. Um tipo $p \in S_m(X)$ é *definível sobre* Y se, para toda fórmula $\phi(v, w)$ de L com v, w seqüências de m, n variáveis respectivamente, existe uma fórmula $d_p\phi(w)$ de L(Y) tal que, para cada $a \in X^n$,

$$\phi(v, a) \in p(v) \Leftrightarrow (\mathfrak{A}, (y)_{y \in Y}) \models d_p\phi(a)\,.$$

(Note que a equivalência refere-se apenas a elementos de X^n.) A associação d_p é chamada *esquema de definição de p*. Quando $X = Y = A$, diremos apenas que p é *definível*.

Observe que, pela definição e quando $X = A$, equivalem em $\mathfrak{A}$ as fórmulas $d_p(\neg\phi)$ e $\neg d_p\phi$, assim como $d_p(\phi \wedge \psi)$ e $d_p\phi \wedge d_p\psi$, e analogamente para outros conectivos.

Note também que dois tipos *sobre o mesmo conjunto* e com o mesmo esquema de definição são, de fato, o mesmo tipo.

Suponha ainda que $Y \subseteq X$. Para cada $a \in X^n$,

$$\big[\, \phi(v, a) \in p(v) \Leftrightarrow \mathfrak{A} \models d_p\phi(a) \,\big] \Leftrightarrow (\phi(v, a) \leftrightarrow d_p\phi(a)) \in p(v)$$

porque $d_p\phi(a)$ é também uma sentença de L(X). Note que esta equivalência é verdadeira independentemente do "significado" de $d_p\phi(a)$, ou seja, de existir um esquema de definição de p.

Exemplo 2.6.2. Suponha $X, Y \subseteq A$, $D \in \mathrm{Def}_X^m$, $a \in A^n$ e $\phi(u, v)$ fórmula de L com u, v seqüências de m, n elementos respectivamente. Seja Δ o conjunto dos elementos das m-uplas de D, também X-definível (para cada uma das m variáveis livres da fórmula que define D, quantifique existencialmente as demais e tome a disjunção dessas fórmulas). Vemos $t(a/\Delta)$ como conjunto de fórmulas tendo as variáveis v livres; assuma que é um tipo definível sobre Y.

Note que $\phi(u, v)$ é uma fórmula a que podemos aplicar seu esquema de definição, obtendo $d_{t(a/\Delta)}\phi(u)$. Suponha $\alpha \in \Delta^m$: então $\mathfrak{A} \models d_{t(a/\Delta)}[\alpha]$ se e somente se a fórmula $\phi(\alpha, v)$ pertence a $t(a/\Delta)$, ou seja, $\mathfrak{A} \models \phi(\alpha, a)$. Assim, $\phi(\mathfrak{A}, a) \cap \Delta^m = d_{t(a/\Delta)}\phi(\mathfrak{A}) \cap \Delta^m$ é um conjunto $Y \cup X$-definível.

Em particular, quando $\phi(\mathfrak{A}, a) \subseteq D$ e aplicamos o próximo corolário, concluímos que $\phi(\mathfrak{A}, a)$ é $\Delta \cup X$-definível.

Corolário 2.6.3. Todo tipo sobre X com posto (ordinal) é definível sobre X.

Demonstração: Podemos supor $p \in S_m^{\mathfrak{C}}(X)$. Tome $D \in \mathrm{Def}^m_{\mathfrak{C},X}$ determinado por p, com $\mathrm{RM}(D) = \mathrm{RM}(p) = \xi$. Então $p = \{E \in \mathrm{Def}^m_{\mathfrak{C},X} \mid D \subseteq_\xi E\}$. Suponha $\phi(v,w)$ fórmula de L como na definição. Pelo Teorema 2.4.3, $\{c \in C^n \mid D \subseteq_\xi \phi(\mathfrak{C}, c)\}$ é definido por uma fórmula $\psi(w)$ de $\mathrm{L}(X)$. Assim, para cada $a \in A^n$,

$$\phi(v,a) \in p(v) \Leftrightarrow D \subseteq_\xi \phi(\mathfrak{C}, a) \Leftrightarrow \mathfrak{C} \models \psi(a) \Leftrightarrow \mathfrak{A} \models \psi(a) .$$

Tome $d_p\phi = \psi$. Note ainda que p é definível sobre um subconjunto finito de X, sobre o qual D é definível. QED

Suponha $\mathfrak{A} \prec \mathfrak{B}$ duas L-estruturas. Trabalharemos somente com tipos *herdeiros* e *globais*, de modo que pospomos o caso geral para a Definição 2.6.9.

Definição 2.6.4. (i) Diz-se que $q \in S_m(B)$ é *herdeiro* de $q|_A$ se, para toda fórmula ϕ de L e todo $b \in B^n$ com $\phi(v,b) \in q(v)$, existe $a \in A^n$ tal que $\phi(v,a) \in q|_A(v)$.

(ii) Diz-se que $q \in S_m(B)$ é *co-herdeiro* de $q|_A$ se, para toda fórmula ϕ de L e todo $b \in B^n$ com $\phi(v,b) \in q(v)$, existe $a \in A^m$ tal que $\mathfrak{B} \models \phi(a,b)$.

Importamos dois comentários de [Poizat 1]:

Primeiramente, esclarecemos a terminologia "herdeiro" — veremos ao fim da seção que "co-herdeiro" é um conceito dual. Suponha que um conjunto de sentenças Σ de uma linguagem estendendo $\mathrm{L}(A)$ com novas constantes tenha esta propriedade de consistência com $p \in S_m(A)$: se c_i, $i \in I$, são seqüências de m novas constantes, então $\Sigma \cup \{p(c_i) \mid i \in I\}$ é consistente. É claro que, nesse caso, Σ tem essa propriedade também com qualquer restrição de p. Porém, se q é um herdeiro de p, Σ tem essa propriedade com q, porque cada subconjunto finito de q (ou uma única fórmula, por conjunção) corresponde a um subconjunto de p, bastando reinterpretar parâmetros. Desse modo, q *herda* propriedades de consistência de p.

Outro termo usado é "primogênito", quando se chamam extensões de "filhos", mas notamos que em geral há muitos herdeiros sobre um mesmo modelo.

Frisemos duas propriedades simples, para as quais suporemos $p \subseteq q \subseteq r$ três tipos globais sobre três estruturas de cadeia elementar. Temos q extensão de p e r de q. Se q é herdeiro de p e r de q, então r é herdeiro de p. Se r é herdeiro de p, então q é herdeiro de p, mas vemos que r não precisa ser herdeiro de q.

Recorremos novamente a [Poizat 1] para adaptar seu Teorema 11.1:

Lema 2.6.5 (Existência). Suponha $p(v) \in S_m(A)$ e $\Phi(v)$ um conjunto de fórmulas de $\mathrm{L}(B)$ fechado sob conjunções, contendo p e tal que, se $\phi(v,b) \in \Phi$

com ϕ fórmula de L e $b \in B^n$, então existe $a \in A^n$ tal que $\phi(v, a) \in p$. Então Φ estende-se a um herdeiro de p sobre B. Em particular, tomando-se $\Phi = p$, vemos que p tem herdeiros sobre B.

Demonstração: Considere o conjunto de fórmulas em Φ e das fórmulas $\neg\psi(v, d)$, em que $d \in B^n$ e ψ é fórmula de L para a qual não existe $a \in A^n$ tal que $\psi(v, a) \in p(v)$.

Mostremos que esse conjunto é consistente com $Th(\mathfrak{B}, (b)_{b \in B})$. Um subconjunto finito seu constitui-se de $\phi_1(v, b_1), \ldots, \phi_r(v, b_r) \in \Phi$ e $\neg\psi_1(v, d_1), \ldots, \neg\psi_s(v, d_s)$ com ϕ_i, ψ_j fórmulas de L. Adicionando novas variáveis às fórmulas originais, podemos tomar todas as constantes de B em conjunto e supor que $b_1 = \ldots = b_r = d_1 = \ldots = d_s$, sem alterar as propriedades dadas por hipótese. Já que $\phi_1(v, b_1) \wedge \ldots \wedge \phi_r(v, b_1) \in \Phi$, existe $a \in A^n$ tal que $\phi_1(v, a) \wedge \ldots \wedge \phi_r(v, a) \in p$. Tome $\mathfrak{C}$ uma extensão elementar de $\mathfrak{B}$ em que p seja realizado por $c \in C^m$. Por hipótese, $\psi_1(v, a), \ldots, \psi_s(v, a) \notin p$, donde $\neg\psi_1(v, a), \ldots, \neg\psi_s(v, a) \in p$ e $\mathfrak{C} \models \phi_1(c, a), \ldots, \phi_r(c, a), \neg\psi_1(c, a), \ldots, \neg\psi_s(c, a)$. Então, interpretando $b_i = d_j$ como a, vemos que o subconjunto finito é consistente com $Th(\mathfrak{B})$, portanto com $Th(\mathfrak{B}, (b)_{b \in B})$ pelo Lema 1.3.10. Pela discussão que antecede o Corolário 1.1.12, concluímos que todo o conjunto é consistente com $Th(\mathfrak{B}, (b)_{b \in B})$.

Então esse conjunto estende-se a um tipo $q \in S_m(B)$. É claro que $\Phi \subseteq q$. Suponha $\phi(v, b) \in q(v)$, com ϕ de L e $b \in B^n$, mas que não exista $a \in A^n$ tal que $\phi(v, a) \in p(v)$. Então $\neg\phi(v, b)$ pertence ao nosso conjunto e então a q consistente, contradição. Obtemos q herdeiro de p. QED

Para caracterizar a unicidade do tipo herdeiro, precisamos do

Teorema 2.6.6 (Beth). Adicione a L novos predicados P_f, n_f-ário, $f \in F$, obtendo a linguagem L$'$. Equivalem:

(i) Suponha $\mathfrak{A}$ uma L-estrutura que, com alguma interpretação $R_f \subseteq A^{n_f}$ para cada P_f, é modelo de uma teoria T' de L$'$. As interpretações R_f são únicas de modo que $(\mathfrak{A}, (R_f)_{f \in F}) \models T'$.

(ii) Cada fórmula atômica P_f equivale em T' a uma fórmula de L.

Referências: O Teorema 2.2.22 de [Chang, Keisler], com pequena adaptação na demonstração, ou o Teorema 6.6.4 de [Hodges], já mais forte. QED

Proposição 2.6.7. Um tipo $p \in S_m(A)$ é definível se e somente se p tem um único herdeiro sobre qualquer extensão elementar de $\mathfrak{A}$. Esse herdeiro tem o mesmo esquema de definição de p.

Demonstração: Suponha p definível e $q \in S_m(B)$ herdeiro de p. Mostraremos que uma fórmula $\phi(v, b)$ pertence a $q(v)$, com ϕ fórmula de L e $b \in B^n$, se e somente se $\mathfrak{B} \models d_p\phi(b)$. Feito isso, notamos que q está perfeitamente caracterizado, sendo portanto único, e que $d_q = d_p$.

Para todo $a \in A^n$, vale $(\phi(v,a) \leftrightarrow d_p\phi(a)) \in p(v)$. Nesse caso, $\neg(\phi(v,a) \leftrightarrow d_p\phi(a)) \notin p(v)$ e, por hipótese, $\neg(\phi(v,b) \leftrightarrow d_p\phi(b)) \notin q(v)$ para todo $b \in B^n$. Assim, para todo $b \in B^n$, vale $(\phi(v,b) \leftrightarrow d_p\phi(b)) \in q(v)$, como desejado.

Suponha agora que p tem um único herdeiro sobre cada extensão elementar de $\mathfrak{A}$. Para cada fórmula $\phi(v,w)$ de L, em que w é seqüência de n_ϕ variáveis e n_ϕ é arbitrário não-nulo, adicione um predicado P_ϕ n_ϕ-ário a L(A) e interprete-o em $\mathfrak{A}$ como $A_\phi = \{a \in A^n \mid \phi(v,a) \in p(v)\}$. Observamos que $A_\phi \cap A_{\neg\phi} = \emptyset$ e $A_\phi \cup A_{\neg\phi} = A^n$. Tome $T' = Th(\mathfrak{A}, (a)_{a\in A}, (A_\phi)_\phi)$.

Se $(\mathfrak{B}, (b_a)_{a\in A}, (B_\phi)_\phi)$ é um modelo de T', podemos considerar $\mathfrak{B}$ extensão elementar de $\mathfrak{A}$ com a identificação $b_a = a$. Mostremos que o conjunto Φ das fórmulas $\phi(v,b)$, em que $\phi(v,w)$ é como acima e $b \in B_\phi$, é um conjunto consistente com $Th(\mathfrak{B}, (b)_{b\in B})$. Suponha $\phi_1(v,b_1), \ldots, \phi_k(v,b_k)$ fórmulas suas: como p é finitamente satisfazível em $\mathfrak{A}$, temos

$$(\mathfrak{A}, (A_\phi)_\phi) \models \forall w_1 \ldots \forall w_k \left(P_{\phi_1}(w_1) \wedge \ldots \wedge P_{\phi_k}(w_k) \rightarrow \right.$$
$$\left. \exists v\, (\phi_1(v,w_1) \wedge \ldots \wedge \phi_k(v,w_k))\right) .$$

Então também $(\mathfrak{B}, (B_\phi)_\phi)$ satisfaz essa sentença e, em particular, $\mathfrak{B} \models \exists v\, (\phi_1(v, b_1) \wedge \ldots \wedge \phi_k(v,b_k))$.

Note que $B_\phi \cap B_{\neg\phi} = \emptyset$ e $B_\phi \cup B_{\neg\phi} = B^n$, de modo que Φ é maximal, ou seja, um tipo. Além disso, Φ contém p: de fato, se $\phi(v,a) \in p(v)$ então $a \in A_\phi \subseteq B_\phi$, donde $\phi(v,a) \in \Phi$. Mas Φ satisfaz a condição da definição de herdeiro: mais precisamente, se $\phi(v,b) \in \Phi$ então $b \in B_\phi$, donde $B_\phi \neq \emptyset$ e existe $a \in A_\phi$, de modo que $\phi(v,a) \in p(v)$. Vemos que o tipo Φ é o herdeiro de p.

Concluímos que cada B_ϕ é o conjunto das n-uplas $b \in B^n$ tais que $\phi(v,b)$ pertence ao único herdeiro de p, ou seja, as interpretações B_ϕ são únicas. Pelo Teorema de Beth, cada $P_\phi(w)$ equivale em T' a uma fórmula $\psi_\phi(w)$ de L(A), donde

$$\phi(v,a) \in p(v) \Leftrightarrow a \in A_\phi \Leftrightarrow (\mathfrak{A}, (A_\phi)_\phi) \models P_\phi(a) \Leftrightarrow \mathfrak{A} \models \psi_\phi(a) .$$

Tome $d_p\phi = \psi_\phi$. QED

Lembramos que, pelo Teorema 2.4.4, tipos globais com posto ordinal sobre estruturas estáveis têm grau 1.

Teorema 2.6.8. Suponha $p \in S_m(A)$ com posto (ordinal) e $q \in S_m(B)$ a única extensão direta de p. Se p determina $D \in \mathrm{Def}^m_{\mathfrak{B},A}$, então q é o único tipo de

$S_m(B)$ com posto RM(p) que contém D. Além disso, q é o único herdeiro de p e tem o mesmo esquema de definição.

Demonstração: Escreva RM$(p) = \xi$ e dM$(p) = 1$. Pela Proposição 2.2.4, D determina $r \in S_m^{\mathfrak{B}}(B)$ o único tipo que contém D com posto RM$(D) = \xi$ e grau dM$(D) = 1$, sendo $r = \{E \in \mathrm{Def}^m_{\mathfrak{B},B} \mid D \subseteq_\xi E\} \supseteq \{E \in \mathrm{Def}^m_{\mathfrak{B},A} \mid D \subseteq_\xi E\} = p$. Assim, r é extensão direta de p, ou seja, $r = q$.

Seja $\mathfrak{C}$ uma extensão elementar $|B|^+$-grande de $\mathfrak{B}$.

Aplicamos agora o Teorema 2.4.3 a $\mathfrak{B}$ em vez de $\mathfrak{A}$. Suponha $\phi(v, w)$ como em seu enunciado e $D(\mathfrak{C})$ o conjunto definido em $\mathfrak{C}$ pela fórmula de L(A) que define D em $\mathfrak{B}$: então $\{c \in C^n \mid D(\mathfrak{C}) \subseteq_\xi \phi(\mathfrak{C}, c)\}$ é definido por uma fórmula $\psi(w)$ de L(A). Assim, para $b \in B^n$, $\mathfrak{B} \models \psi(b) \Leftrightarrow \mathfrak{C} \models \psi(b) \Leftrightarrow$ RM$(D(\mathfrak{C}) - \phi(\mathfrak{C}, b)) < \xi \Leftrightarrow$ RM$(D - \phi(\mathfrak{B}, b)) < \xi \Leftrightarrow \phi(\mathfrak{B}, b) \in r = q$. Tome $d_q\phi = \psi$, de modo que q é definível.

Contudo, vimos no Corolário 2.6.3 que p é definível, e a Proposição 2.6.7 então garante que p tem um único herdeiro sobre $\mathfrak{B}$, com o mesmo esquema de definição d_p. Basta mostrar então que d_q é esse esquema, de modo que o herdeiro será igual a q. Como vimos, ψ é fórmula de L(A): então, para $a \in A^n$, $\phi(v, a) \in p(v) \Leftrightarrow \phi(v, a) \in q(v) \Leftrightarrow \mathfrak{B} \models d_q\phi(a) \Leftrightarrow \mathfrak{A} \models d_q\phi(a)$, donde podemos tomar $d_p = d_q$. QED

Sabe-se ainda que, por simetria, q também é o único co-herdeiro de p.

A título de completude, apresentamos a definição geral de tipos herdeiros, embora sua restrição deva ser global.

Suponha $\mathfrak{A}$ uma L-estrutura e Y um conjunto contendo A. Pelo Teorema de Löwenheim–Skolem e providenciando-se as colagens isomorfas de praxe, sempre existe uma extensão elementar $\mathfrak{C}$ de $\mathfrak{A}$ com $Y \subseteq C$. Para considerar tipos sobre Y, é preciso especificar a estrutura $\mathfrak{C}$ à qual (e a $Th(\mathfrak{C}, (y)_{y \in Y})$) referem-se afirmações de consistência. Supomos então $\mathfrak{C}$ um modelo monstro, sem grandeza específica, e assumimos que as extensões elementares de $\mathfrak{A}$ contendo Y são subestruturas de $\mathfrak{C}$ — note que não se trata de universalidade de $\mathfrak{C}$, pela qual se obtém apenas imersão.

Definição 2.6.9. (i) Diz-se que $q \in S_m(Y)$ é *herdeiro* de $q|_A$ se se estende a um herdeiro de $q|_A$ sobre qualquer extensão elementar de $\mathfrak{A}$ contendo Y.

(ii) Diz-se que $q \in S_m(Y)$ é *co-herdeiro* de $q|_A$ se se estende a um co-herdeiro de $q|_A$ sobre qualquer extensão elementar de $\mathfrak{A}$ contendo Y.

A mudança na definição é apenas aparente:

Proposição 2.6.10. (i) $q \in S_m(Y)$ é herdeiro de $q|_A$ se e somente se, para toda fórmula ϕ de L e todo $y \in Y^n$ com $\phi(v, y) \in q(v)$, existe $a \in A^n$ tal que $\phi(v, a) \in q|_A(v)$.

(ii) $q \in S_m(Y)$ é co-herdeiro de $q|_A$ se e somente se, para toda fórmula ϕ de L, todo $y \in Y^n$ com $\phi(v, y) \in q(v)$ e toda extensão elementar $\mathfrak{B}$ de $\mathfrak{A}$ contendo Y, existe $a \in A^m$ tal que $\mathfrak{B} \models \phi(a, y)$.

Demonstração: (i) Para a implicação direta, tome $\mathfrak{B}$ extensão elementar de $\mathfrak{A}$ com $Y \subseteq B$ e aplique a definição. Para a recíproca, dada $\mathfrak{B}$ nessas condições, use o lema de existência, cujas hipóteses já são verificadas.

(ii) A implicação direta é demonstrada pelo mesmo argumento de (i). Para a recíproca, um resultado correspondente de existência pode ser usado do mesmo modo e encontrado nos Lemas 12.10 e 12.11 de [Poizat 1]. QED

Corolário 2.6.11 (Dualidade). Suponha c, d seqüências de elementos de C com m, n elementos, respectivamente. Então $t(c/Ad)$ é herdeiro de $t(c/A)$ se e somente se $t(d/Ac)$ é co-herdeiro de $t(d/A)$.

Demonstração: Podemos trabalhar com fórmulas de L(A), inserindo sempre todos os parâmetros de A já nas fórmulas. Assim, não precisamos contar outros parâmetros em A e podemos supor que seqüências sobre Ac ou Ad são as próprias c ou d respectivamente.

Pelo item (i), $t(c/Ad)$ é herdeiro de $t(c/A)$ se e somente se, para toda fórmula ϕ de L(A) tal que $\mathfrak{C} \models \phi(c, d)$, existe $a \in A^n$ tal que $\mathfrak{C} \models \phi(c, a)$.

Pelo item (ii), $t(d/Ac)$ é co-herdeiro de $t(d/A)$ se e somente se, para toda fórmula ψ de L tal que $\mathfrak{C} \models \psi(d, c)$ e toda extensão elementar $\mathfrak{B}$ de $\mathfrak{A}$ contendo Ac, existe $a \in A^m$ tal que $\mathfrak{B} \models \psi(a, c)$. Mas $\mathfrak{C}$ é uma tal extensão, e basta verificar a condição quanto a $\mathfrak{C}$ por hipótese — supomos toda $\mathfrak{B}$ subestrutura de $\mathfrak{C}$.

Basta então tomar ϕ e ψ obtidas uma de outra permutando suas variáveis.

QED

3

Geometria do fecho algébrico

Como no capítulo anterior, trabalharemos com uma linguagem arbitrária L e outras condições serão particulares a cada seção. Também permanece válida nossa nota sobre a redação e as influências de [Ziegler], [Pillay] e [Hodges].

Introduziremos o operador mais utilizado neste texto e em boa parte da Teoria dos Modelos: o fecho algébrico acl($\cdot$), cujas principais propriedades são conseqüências da formulação de L em primeira ordem. Estudaremos, em seqüência, sua relação com automorfismos, suas propriedades gerais com o posto de Morley, seu comportamente enquanto fecho combinatório em conjuntos fortemente minimais, e as noções de dimensão e independência resultantes. Identificaremos, sob condições precisas, a independência sob este fecho e a independência de deviação que estudamos anteriormente.

3.1. Fechos definível e algébrico

Deveremos deduzir algumas propriedades antes de apresentar exemplos. Sejam $\mathfrak{A}$ uma L-estrutura e $X, Y \subseteq A$.

Embora apresentemos esta definição diretamente para o grupo de automorfismos sobre X, ela pode ser adaptada para qualquer (subgrupo de) grupo de permutações, como em [Hodges]. Seguiremos sua distinção maiúscula.

Definição 3.1.1. DCL(X) é o conjunto dos elementos de A fixados pelos automorfismos sobre X.

ACL(X) é o conjunto dos elementos de A com número finito de imagens pelos automorfismos sobre X, chamadas *X-conjugados*.

Proposição 3.1.2. (i) $X \subseteq \mathrm{DCL}(X) \subseteq \mathrm{ACL}(X)$.

(ii) Se $X \subseteq Y$ então $\mathrm{DCL}(X) \subseteq \mathrm{DCL}(Y)$ e $\mathrm{ACL}(X) \subseteq \mathrm{ACL}(Y)$.

(iii) Se $X \subseteq \mathrm{DCL}(Y)$ então $\mathrm{DCL}(X) \subseteq \mathrm{DCL}(Y)$.

(iv) $\mathrm{DCL}(\mathrm{DCL}(X)) = \mathrm{DCL}(X)$.

Demonstração: Os fatos (i) e (ii) seguem da definição.

Suponha $a \in \mathrm{DCL}(X)$ e $X \subseteq \mathrm{DCL}(Y)$. Por definição, um automorfismo sobre Y fixa os elementos de X e é, então, um automorfismo sobre X. Portanto, esse automorfismo fixa a. Concluímos que $a \in \mathrm{DCL}(Y)$ e obtemos (iii).

Demonstremos (iv). Por (i), temos $X \subseteq \mathrm{DCL}(X)$, e a propriedade (ii) implica $\mathrm{DCL}(X) \subseteq \mathrm{DCL}(\mathrm{DCL}(X))$. Também temos $\mathrm{DCL}(X) \subseteq \mathrm{DCL}(X)$, a que se aplica a afirmação (iii) para obter $\mathrm{DCL}(\mathrm{DCL}(X)) \subseteq \mathrm{DCL}(X)$. QED

Faremos agora a definição e as deduções centrais desta seção.

Definição 3.1.3. (i) O *fecho definível de* X é o conjunto $\mathrm{dcl}(X)$ dos elementos X-definíveis. (Em inglês, dcl abrevia *definable/definitional closure.*) *Atenção:* ***não*** *se trata de um menor conjunto definível que contenha* X.

(ii) Elementos de conjuntos X-definíveis finitos são ditos *algébricos sobre* X. Indique $\mathrm{acl}(X)$ o *fecho algébrico de* X, conjunto dos algébricos sobre X. (Em inglês, acl abrevia *algebraic closure.*)

Fato 3.1.4. $\mathrm{dcl}(X)$ e $\mathrm{acl}(X)$ são os mesmos em qualquer extensão (ou subestrutura que contenha X) elementar de $\mathfrak{A}$.

Porque a elementaridade preserva o número de elementos de um X-definível finito.

Fato 3.1.5. $\mathrm{dcl}(X) \subseteq \mathrm{DCL}(X)$ e $\mathrm{acl}(X) \subseteq \mathrm{ACL}(X)$.

Demonstração: Suponha que ξ seja um automorfismo de $\mathfrak{A}$ e D um subconjunto definível de A^m com ϕ uma fórmula de L e $a \in A^n$ tais que $D = \phi(\mathfrak{A}, a)$. Vimos que $\xi[D] = \phi(\mathfrak{A}, \xi(a))$. Caso ξ seja um automorfismo sobre X e a seja uma seqüência de parâmetros de X, temos $\xi(a) = a$ e $\xi[D] = D$. QED

Proposição 3.1.6. (i) $X \subseteq \mathrm{dcl}(X) \subseteq \mathrm{acl}(X)$.

(ii) Se $X \subseteq Y$ então $\mathrm{dcl}(X) \subseteq \mathrm{dcl}(Y)$ e $\mathrm{acl}(X) \subseteq \mathrm{acl}(Y)$.

(iii) Se $X \subseteq \mathrm{dcl}(Y)$ então $\mathrm{dcl}(X) \subseteq \mathrm{dcl}(Y)$; analogamente quanto a $\mathrm{acl}(\cdot)$.

(iv) $\mathrm{dcl}(\mathrm{dcl}(X)) = \mathrm{dcl}(X)$ e $\mathrm{acl}(\mathrm{acl}(X)) = \mathrm{acl}(X)$.

(v) Para todo $a \in \mathrm{dcl}(X)$ existe X_0 subconjunto finito de X tal que $a \in \mathrm{dcl}(X_0)$; analogamente quanto a $\mathrm{acl}(\cdot)$.

Demonstração: Novamente, (i) e (ii) seguem da definição.

Consideramos (iii), (iv), (v) primeiro quanto a $\mathrm{dcl}(\cdot)$:

Para provar (iii), suponha $a \in \mathrm{dcl}(X)$ e $X \subseteq \mathrm{dcl}(Y)$. Existem $\phi(v, v_1, \ldots, v_n)$ fórmula de L, $x_1, \ldots, x_n \in X$ e fórmulas $\phi_1, \ldots, \phi_n$ de $\mathrm{L}(Y)$ com $\{a\} = \phi(\mathfrak{A}, x_1, \ldots, x_n)$ e cada $\{x_i\} = \phi_i(\mathfrak{A}, (y)_{y \in Y})$. Então

$$\exists v_1 \ldots \exists v_n \left(\phi(v, v_1, \ldots, v_n) \wedge \bigwedge_{i=1}^{n} \phi_i(v_i)\right)$$

define a com parâmetros em Y. O definível é realmente unitário porque apenas $(x_1, \ldots, x_n)$ satisfaz $\bigwedge_{i=1}^{n} \phi_i(v_i)$ interpretando as variáveis adequadamente.

Consideremos (iv). Por (i), temos $X \subseteq \mathrm{dcl}(X)$, e então (ii) implica $\mathrm{dcl}(X) \subseteq \mathrm{dcl}(\mathrm{dcl}(X))$. Também temos $\mathrm{dcl}(X) \subseteq \mathrm{dcl}(X)$, a que se aplica a propriedade (iii) para obter $\mathrm{dcl}(\mathrm{dcl}(X)) \subseteq \mathrm{dcl}(X)$.

O fato (v) segue da definição: dado $a \in \mathrm{dcl}(X)$, existe uma fórmula com parâmetros em X que é satisfeita somente por a; tome X_0 o conjunto finito dos parâmetros de X que ocorrem nessa fórmula.

Agora, os enunciados quanto a $\mathrm{acl}(\cdot)$:

Para (iii), o raciocínio correspondente deve ser mais elaborado. Suponha $a \in \mathrm{acl}(X)$ e $X \subseteq \mathrm{acl}(Y)$. Existem $\phi(v, v_1, \ldots, v_n)$ fórmula de L, $x_1, \ldots, x_n \in X$ e fórmulas $\phi_1, \ldots, \phi_n$ de L(Y) com $a \in \phi(\mathfrak{A}, x_1, \ldots, x_n)$ *finito* e cada $x_i \in \phi_i(\mathfrak{A}, (y)_{y \in Y})$ *finito*. Porém, $\phi(\mathfrak{A}, b_1, \ldots, b_n)$ pode não ser finito para alguns $b_1, \ldots, b_n \in \mathrm{acl}(Y)$.

Suponha que $\phi(\mathfrak{A}, x_1, \ldots, x_n)$ tenha k elementos e cada $\phi_i((\mathfrak{A}, (y)_{y \in Y}))$ tenha k_i elementos. Considere o conjunto definido por

$$\exists v_1 \ldots \exists v_n \left(\phi(v, v_1, \ldots, v_n) \wedge \exists^{\leqslant k} u\, \phi(u, v_1, \ldots, v_n) \wedge \bigwedge_{i=1}^{n} \phi_i(v_i) \right) .$$

Para a variável v_i, temos k_i possibilidades de satisfação de $\phi_i(v_i)$, de modo que há $k_1 \ldots k_n$ possibilidades, de início, para interpretar as variáveis $v_1, \ldots, v_n$. Entretanto, $\exists^{\leqslant k} u\, \phi(u, v_1, \ldots, v_n)$ garante que o conjunto definido por ϕ com tais parâmetros tem $\leqslant k$ elementos, de modo que o definível tem *no máximo* $k k_1 \ldots k_n$ elementos. Mas, interpretando cada v_i como x_i, vemos que a pertence a esse definível.

A prova de (iv) é análoga àquela para $\mathrm{dcl}(\cdot)$. Na prova de (v), substitua a satisfação somente por a pela satisfação por um número finito de elementos, dentre os quais a. QED

Comparemos estes fechos quando as estruturas são corpos e a linguagem é a dos anéis com unidade (apenas). Lembre que, se L é um corpo, $X \subseteq L$ e K é o subcorpo gerado por X, então os automorfismos de L sobre X são precisamente aqueles sobre K, donde $\mathrm{DCL}(X) = \mathrm{DCL}(K)$ e $\mathrm{ACL}(X) = \mathrm{ACL}(K)$. Por outro lado, sabemos que $\mathrm{Def}^1_{L,K} = \mathrm{Def}^1_{L,X}$ e vem $\mathrm{dcl}(X) = \mathrm{dcl}(K)$ e $\mathrm{acl}(X) = \mathrm{acl}(K)$. Assim, contentamo-nos em trabalhar diretamente com o subcorpo K. O primeiro exemplo estuda a extensão cotidiana $\mathbb{Q} \subseteq \mathbb{R}$ e o segundo apresenta o importante caso em que L é algebricamente fechado.

Exemplo 3.1.7. O único automorfismo do corpo $\mathbb{R}$ sobre $\mathbb{Q}$ é a identidade, de modo que $\mathrm{DCL}(\mathbb{Q}) = \mathrm{ACL}(\mathbb{Q}) = \mathbb{R}$. Primeiramente, notamos que a ordem usual é $\emptyset$-definível em $\mathbb{R}$ porque $x \leqslant y \Leftrightarrow \mathbb{R} \models \exists v\, (x + v^2 = y)$, de modo que todo autormofismo de $\mathbb{R}$ sobre $\mathbb{Q}$ é crescente. Agora, suponha ξ um tal automorfismo e $x \in \mathbb{R}$ com, digamos, $x < \xi(x)$: então existe $r \in \mathbb{Q}$ com $x < r < \xi(x) < \xi(r) = r$, contradição.

Seja agora $\phi(x, w)$ uma fórmula com x variável e w seqüência de n variáveis. Seja também $a \in \mathbb{Q}^n$ e suponha que $\phi(\mathbb{R}, a)$ é um conjunto finito com $k \geqslant 2$ elementos, que se ordenam $x_1 < \ldots < x_k$. Então existem $r_1, \ldots, r_{k-1} \in \mathbb{Q}$ com $x_1 < r_1 < x_2 < \ldots < r_{k-1} < x_k$. Com os novos parâmetros r_j, podemos definir cada x_i, novamente porque a ordem é $\emptyset$-definível. Por exemplo, a fórmula $\phi(x, a) \wedge \exists v\, (x + v^2 = r_1)$ tem parâmetros em $\mathbb{Q}$ e é satisfeita apenas por x_1. Concluímos que $\operatorname{acl}(\mathbb{Q}) = \operatorname{dcl}(\mathbb{Q})$.

Considere o corpo $\mathbb{Q}^{\mathrm{r}}$ dos números reais algébricos (sobre $\mathbb{Q}$): mostraremos que $\operatorname{dcl}(\mathbb{Q}) = \operatorname{acl}(\mathbb{Q}) = \mathbb{Q}^{\mathrm{r}}$. Para tanto, faremos uso de conceitos pertinentes à teoria dos corpos reais fechados, que não exporemos porque não tornaremos a vê-los; contudo, trata-se de um conceito importante em Álgebra e também em Teoria dos Modelos. (Referências em Álgebra são o Capítulo XI de [Lang] e o Capítulo 11 de [Jacobson II].) Um corpo *real fechado* é um corpo ordenado em que todo polinômio de uma variável de grau ímpar tem raiz e todo elemento positivo tem raiz quadrada, ou seja, a ordem é definível como em $\mathbb{R}$. Vemos então que $\mathbb{Q}^{\mathrm{r}}$ e $\mathbb{R}$ são corpos reais fechados. Essa teoria tem eliminação de quantificadores na linguagem dos anéis com unidade e ordem, como mostram o Teorema 8.4.4 de [Hodges] ou o Teorema 3.3.15 de [Marker], de modo que $\mathbb{Q}^{\mathrm{r}} \prec \mathbb{R}$.

A eliminação de quantificadores não se estende à linguagem dos anéis com unidade, embora a ordem seja definível. De fato, se assim fosse, $\mathbb{R}$ seria uma estrutura minimal pela demonstração do Exemplo 1.3.6, porém a fórmula $\exists v\, (x = v^2)$ define um conjunto (dos reais positivos ou 0) infinito com complemento infinito. Contudo, a ordem ser definível implica que os conjuntos definíveis são os mesmos em ambas as linguagens.

Aqui, é mais importante que também na linguagem dos anéis com unidade a extensão $\mathbb{Q}^{\mathrm{r}} \prec \mathbb{R}$ é elementar, porque as fórmulas desta linguagem são fórmulas da outra. Assim, considere ainda $\operatorname{acl}(\mathbb{Q})$ fecho na linguagem original.

Suponha $a \in \mathbb{Q}^{\mathrm{r}}$ com polinômio minimal $m \in \mathbb{Q}[x]$. Então m tem um número finito de raízes e escreve-se a fórmula $m(x) = 0$ com parâmetros em $\mathbb{Q}$, de modo que $a \in \operatorname{acl}(\mathbb{Q})$. Assim, $\mathbb{Q}^{\mathrm{r}} \subseteq \operatorname{acl}(\mathbb{Q})$. Contudo, como $\mathbb{Q}^{\mathrm{r}}$ é subestrutura elementar de $\mathbb{R}$, o fecho é o mesmo em ambas as estruturas, de modo que $\operatorname{acl}(\mathbb{Q}) \subseteq \mathbb{Q}^{\mathrm{r}}$.

Exemplo 3.1.8. Suponha L um corpo algebricamente fechado e K um subcorpo de L. Mostraremos que $\operatorname{acl}(K) = \operatorname{ACL}(K)$ igual ainda ao fecho algébrico de K em L e que $\operatorname{dcl}(K) = \operatorname{DCL}(K)$ igual ainda ao fecho perfeito de K em L.

O fecho algébrico de K em L é, por definição, o subcorpo de L dos elementos algébricos sobre K. Como L é algebricamente fechado, trata-se também de um fecho algébrico (usual) de K porque é uma extensão algébrica. Suponha $a \in L$ algébrico sobre K e seja $m \in K[x]$ seu polinômio minimal. Então m tem um número finito de raízes em L e $m(v) = 0$ é uma fórmula com parâmetros em K, de modo que $a \in \mathrm{acl}(K)$. Sabemos que $\mathrm{acl}(K) \subseteq \mathrm{ACL}(K)$, fato que agora percebemos generalizar este raciocínio algébrico: sendo ξ um automorfismo de L sobre K, temos também $m(\xi(a)) = \xi(m(a)) = \xi(0) = 0$ e $\xi(a)$ raiz de m.

Basta, portanto, mostrar que o fecho algébrico de K em L contém $\mathrm{ACL}(K)$. Suponha agora $a \in L$ transcendente sobre K. Lembramos que então existe um número infinito de transcendentes sobre K, por exemplo, a^n para cada $n \in \mathbb{N}^*$ (são distintos porque se $a^i = a^j$ com $i > j$ então $a^{i-j} - 1 = 0$). Mas, para cada $b \in L$ transcendente sobre K, vimos na Seção 1.2 que existe um automorfismo de L sobre K que leva a a b. Assim, a tem um número infinito de conjugados e $a \notin \mathrm{ACL}(K)$. A título de curiosidade, lembramos que todos os transcendentes de L sobre K têm o mesmo tipo sobre L, e então satisfazem precisamente as mesmas fórmulas com parâmetros em L ou somente K, concluindo-se diretamente que $a \notin \mathrm{acl}(K)$.

O fecho perfeito de K em L é, também por definição, o menor subcorpo perfeito de L que contém K — como L é algebricamente fechado, é perfeito. Suponha L com característica $p > 0$ e defina $K^{p^{-n}} = (\varphi^n)^{-1}[K]$, em que φ é a função de Frobenius $\varphi(x) = x^p$, e $K^{p^{-\infty}} = \bigcup_{n \in \mathbb{N}} K^{p^{-n}}$. A condição de sobrejetividade de φ e sua injetividade implicam que a intersecção de corpos perfeitos é ainda perfeita; como L é perfeito, existe realmente o fecho perfeito F de K em L. Mostremos que $F = K^{p^{-\infty}} = \{a \in L \mid a^{p^n} \in K \text{ para algum } n \in \mathbb{N}\}$. Se $\varphi^n(a) \in K \subseteq F$ então, por φ^n ser sobrejetora em F e também injetora, temos $a \in F$. Por outro lado, $(K^{p^{-n}})_{n \in \mathbb{N}}$ é uma cadeia de corpos, verificando-se que $K^{p^{-\infty}}$ é um corpo contendo K e bastando provar que $K^{p^{-\infty}}$ é perfeito. Dado $a \in K^{p^{-\infty}}$, temos $a^{p^n} \in K$ para algum $n \in \mathbb{N}$, existindo $b \in L$ com $b^p - a = 0$ já que L é algebricamente fechado. Então $\varphi(b) = a$ e $b^{p^{n+1}} = a^{p^n} \in K$, donde $b \in K^{p^{-\infty}}$.

Observamos, em qualquer característica, que todo elemento de $\mathrm{DCL}(K)$ é algébrico sobre K, porque $\mathrm{DCL}(K) \subseteq \mathrm{ACL}(K)$. Mostraremos inicialmente que $\mathrm{DCL}(K)$ é o conjunto dos elementos $a \in L$ algébricos sobre K com polinômio minimal $m \in K[x]$ com raiz única a, ou seja, multiplicidade igual ao grau de m. Suponha $a \in L$ algébrico sobre K e $m \in K[x]$ seu polinômio minimal: todos os conjugados de a são raízes de m. Se a é a única raiz, então imediatamente $a \in \mathrm{DCL}(K)$. Se $b \in L$ é uma raiz distinta, vimos na Seção 1.2 que existe um automorfismo de L sobre K que leva a a b, donde $a \notin \mathrm{DCL}(K)$.

Desse modo, no caso de característica 0 e K já ser perfeito, um elemento de

$\mathrm{DCL}(K)$ tem polinômio minimal com grau 1, de modo que pertence a K. De $K \subseteq \mathrm{dcl}(K) \subseteq \mathrm{DCL}(K)$, concluímos a igualdade dos três conjuntos.

No caso de característica $p > 0$ e $F = K^{p^{-\infty}}$ o fecho perfeito de K em L, notamos que o polinômio minimal sobre K de $a \in \mathrm{DCL}(K)$ é divisível pelo minimal sobre F, que portanto também tem a como única raiz. Novamente, por F ser perfeito, este minimal tem grau 1 e $a \in F$. Por outro lado, se $a \in F$ então $\varphi^n(a) \in K$ para algum $n \in \mathbb{N}$, mas como φ^n é uma função injetora e $\emptyset$-definível, obtemos $a \in \mathrm{dcl}(K)$. Finalmente, lembramos que $\mathrm{dcl}(K) \subseteq \mathrm{DCL}(K)$.

Façamos algumas colocações adicionais, também a título de curiosidade, para característica $p > 0$. Obtivemos $\mathrm{dcl}(K) = \mathrm{DCL}(K) = K^{p^{-\infty}} = \{a \in L \,|\, a^{p^n} \in K$ para algum $n \in \mathbb{N}\}$. Há um raciocínio direto: se ξ é um automorfismo de L sobre K e $a^{p^n} \in K$, então $a^{p^n} = \xi(a^{p^n}) = (\xi(a))^{p^n}$; por injetividade da função de Frobenius, $a = \xi(a)$ e $a \in \mathrm{DCL}(K)$. Além disso, $\mathrm{dcl}(K) \subseteq \mathrm{dcl}(F)$ porque F é extensão de K. Assim, se $a \in \mathrm{dcl}(K)$ então $t(a/F)$ é isolado pelo conjunto F-definível das raízes do polinômio minimal m de a sobre F. Se m tem outras raízes, todas têm o mesmo tipo $t(a/F)$, o que contradiz $a \in \mathrm{dcl}(F)$. Conclui-se diretamente que m tem a como única raiz, com grau 1, e que $a \in F$.

Para generalizar as equivalências deste exemplo, devemos trabalhar em um modelo monstro κ-grande $\mathfrak{C}$, com $\kappa > |\mathrm{L}|$ e $X \subseteq C$ satisfazendo $|X| < \kappa$. Observamos que $|\mathrm{L}(X)| < \kappa$ implica $|\mathrm{dcl}(X)|, |\mathrm{acl}(X)| < \kappa$, o que nos permite tratar $\mathrm{dcl}(X)$ e $\mathrm{acl}(X)$ como conjuntos de parâmetros também.

Proposição 3.1.9. Nessas condições, $\mathrm{dcl}(X) = \mathrm{DCL}(X)$ e $\mathrm{acl}(X) = \mathrm{ACL}(X)$, ou seja,

(i) $a \in \mathrm{dcl}(X) \Leftrightarrow$ todo automorfismo sobre X fixa a.

(ii) $a \in \mathrm{acl}(X) \Leftrightarrow a$ tem apenas um número finito de X-conjugados.

Demonstração: Basta aplicar o Corolário 1.4.7: o item (i) é dado pelo enunciado sobre a m-upla a, para $m = 1$; o item (ii) é dado pelo enunciado sobre subconjuntos finitos, como o dos X-conjugados de a. QED

Finalmente, notamos que o Exemplo 1.3.1 generaliza-se, com o mesmo raciocínio, à igualdade $\mathrm{Def}^m_{\mathrm{dcl}(X)} = \mathrm{Def}^m_X$ e, então, à identificação $S_m(\mathrm{dcl}(X)) = S_m(X)$.

3.2. Relações com o posto de Morley

O posto de Morley de um tipo tem propriedades especiais quando ocorrem relações com o fecho algébrico.

Considere ainda $\mathfrak{A}$ arbitrária e $X \subseteq A$. Suponha $a = (a_1, \ldots, a_m) \in A^m$ com $m \neq 0$.

Temos $\mathrm{RM}(a/X) = 0 \Leftrightarrow a_1, \ldots, a_m \in \mathrm{acl}(X)$. Isso ocorre porque 0 é o menor posto que um tipo pode ter, precisamente quando contém um definível D de posto 0, ou seja, finito; neste caso, as projeções de D em cada uma de suas m "coordenadas" são ainda definíveis finitos sobre os mesmos parâmetros, e reciprocamente seu produto é finito. Analogamente, no caso de posto nulo, $\mathrm{dM}(a/X)$ é a menor cardinalidade de um tal D.

Proposição 3.2.1. Suponha ainda $b = (b_1, \ldots, b_n) \in A^n$ com cada $b_i \in \mathrm{acl}(Xa)$: então $\mathrm{RM}(a, b/X) = \mathrm{RM}(a/X)$. Em geral, por permutações $\emptyset$-definíveis, podemos supor a_i, b_j em qualquer seqüência.

Demonstração: Note que podemos assumir $n = 1$, pois em geral bastará retirar n elementos.

Pela Proposição 2.2.2, já temos $\mathrm{RM}(a/X) \leqslant \mathrm{RM}(a, b/X)$. Provaremos por indução em um ordinal ξ que $\mathrm{RM}(a, b/X) \geqslant \xi$ implica $\mathrm{RM}(a/X) \geqslant \xi$, concluindo que $\mathrm{RM}(a, b/X) \leqslant \mathrm{RM}(a/X)$. Os casos de ordinal 0 e limite sendo imediatos, como de costume, assumimos a hipótese para o ordinal ξ, em qualquer estrutura e com qualquer conjunto de parâmetros, e consideramos o caso $\xi + 1$. Suponha que $\mathrm{RM}(a, b/X) \geqslant \xi + 1 > \xi$, de modo que $\mathrm{RM}(a/X) \geqslant \xi$. Procedendo por redução ao absurdo, suponha $\mathrm{RM}(a/X) = \xi$.

Tome uma extensão elementar ω-saturada $\mathfrak{B}$ de $\mathfrak{A}$. Sejam ϕ, ψ fórmulas de $\mathrm{L}(X)$ tais que $\phi(\mathfrak{B}) \in t_{\mathfrak{B}}(a/X)$ com posto ξ e $\mathfrak{A}$ satisfaz $\psi(a, b)$ e $\exists^{=r} w\, \psi(a, w)$. Considere a fórmula também de $\mathrm{L}(X)$

$$\phi'(v, w) : \phi(v) \wedge \psi(v, w) \wedge \exists^{=r} u\, \psi(v, u) \,.$$

Então $\mathfrak{B} \models \phi'[a, b]$ e $\mathrm{RM}(\phi'(\mathfrak{B})) \geqslant \xi + 1$. Porque $\mathfrak{B}$ é ω-saturada, pelo Lema 2.1.10 existem fórmulas θ_i de $\mathrm{L}(B)$, $i \in \mathbb{N}$, tais que $\theta_i(\mathfrak{B})$ são dois a dois disjuntos contidos em $\phi'(\mathfrak{B})$ e com posto $\geqslant \xi$. Tome $\chi_i(v) : \exists w\, \theta_i(v, w)$, de modo que χ_i implica ϕ.

Tome $\mathfrak{C}$ uma extensão elementar κ-grande de $\mathfrak{B}$, com $\kappa > |\mathrm{L}|, |B|$. Para cada $i \in \mathbb{N}$, algum tipo a que θ_i pertence tem o mesmo posto, pela Proposição 2.2.5, e é realizado por (c_i, d_i), $c_i \in C^n$ e $d_i \in C$. Desse modo, $\mathrm{RM}(c_i, d_i/B) \geqslant \xi$ e, por hipótese de indução neste caso, $\mathrm{RM}(c_i/B) \geqslant \xi$. Como $\mathfrak{C} \models \chi_i[c_i]$, concluímos que $\mathrm{RM}(\chi_i(\mathfrak{C})) \geqslant \xi$. Mas, por realizar θ_i, a seqüência (c_i, d_i) satisfaz também ϕ', de modo que $d_i \in \mathrm{acl}(Xc_i) \subseteq \mathrm{acl}(Bc_i)$.

Particione $\phi(\mathfrak{C}) = D_1 \cup \ldots \cup D_{\mathrm{dM}(\phi(\mathfrak{C}))}$ dois a dois disjuntos B-definíveis de posto ξ e grau 1 ($\mathfrak{B}$ é ω-saturada). Para cada índice i, como $\chi_i(\mathfrak{C}) \subseteq \phi(\mathfrak{C})$, ambos os conjuntos têm posto ξ e existe um índice j tal que $D_j \cap \chi_i(\mathfrak{C})$ tem posto ξ, donde $D_j - \chi_i(\mathfrak{C})$ tem posto $< \xi$. Para algum j, isso ocorre para infinitos índices i, já que $1 \leqslant j \leqslant \mathrm{dM}(\phi(\mathfrak{C})) < \omega$ e $i \in \mathbb{N}$. Neste caso, para qualquer conjunto finito I_0 de tais índices, temos $\bigcup_{i\in I_0}(D_j - \chi_i(\mathfrak{C}))$ com posto $< \xi$ e então $D_j \cap \bigcap_{i\in I_0} \chi_i(\mathfrak{C})$ tem posto ξ e, em particular, é não-vazio.

Como $\kappa > |\mathrm{L}|, |B|$, podemos aplicar o item (iv) da Proposição 1.4.2 e concluir que a intersecção dos conjuntos $\chi_i(\mathfrak{C})$ para uma família infinita de índices i é não-vazia. Para simplicidade de notação, suponha que já se trata de todo o conjunto-índice $\mathbb{N}$. Assim, existe $c \in C^n$ tal que $\mathfrak{C} \models \chi_i(c)$ para todo $i \in \mathbb{N}$ e, para cada i, existe d_i tal que $\mathfrak{C} \models \theta_i[c, d_i]$. Como os $\theta_i(\mathfrak{C})$ são dois a dois disjuntos, os d_i são distintos. Mas $\theta_i(\mathfrak{C}) \subseteq \phi'(\mathfrak{C})$. Assim, $\mathfrak{C} \models \psi(c, d_i)$ para cada i, contradizendo $\mathfrak{C} \models \exists^{=r} w\, \psi(c, w)$. QED

Corolário 3.2.2. Nas mesmas condições, $\mathrm{RM}(b/X) \leqslant \mathrm{RM}(a/X)$.

Temos $\mathrm{RM}(b/X) \leqslant \mathrm{RM}(a, b/X) = \mathrm{RM}(a/X)$.

Proposição 3.2.3. Um tipo sobre $\mathrm{acl}(X)$ não se desvia sobre X.

Demonstração: Podemos supor que o tipo em questão é principal, já que seu posto e o fecho algébrico independem da extensão elementar em que são calculados. Considere $t(a/\mathrm{acl}(X))$. Cada seqüência finita não-vazia x de elementos de $\mathrm{acl}(X)$ satisfaz $\mathrm{RM}(x/Xa) = 0 = \mathrm{RM}(x/X)$, ou seja, x independe de a sobre X. Por definição, $\mathrm{acl}(X) \mathop{\perp}_X a$ e, por simetria, $a \mathop{\perp}_X \mathrm{acl}(X)$, como desejado. QED

3.3. Pré-geometrias

Um dos tópicos da Combinatória é a teoria das pré-geometrias ou matróides e geometrias (combinatórias) ou matróides simples. O objetivo é estudar a relação de fecho em seu aspecto "gerador": o exemplo prototípico são os espaços vetoriais com o conceito de combinação linear.

Duas referências dessa área da Combinatória são os livros de H. H. Crapo, G.-C. Rota, *On the Foundations of Combinatorial Theory: Combinatorial Geometries*, edição preliminar, The M.I.T. Press, 1970, e D. J. A. Welsh, *Matroid Theory*, Academic Press, 1976.

Esta seção é basicamente expositória, e o leitor pode preferir lê-la por alto, prosseguir na próxima seção — em que se estuda o fecho algébrico $\mathrm{acl}(\cdot)$ por esta teoria —, e retornar para consultar os pré-requesitos necessários.

Embora este material não se relacione diretamente com as noções geométricas de curvas algébricas, que objetivamos estudar, veremos ser apenas uma impressão inicial.

Definição 3.3.1. Sejam G um conjunto qualquer não-vazio, $P(G)$ o conjunto dos subconjuntos de G e $\mathrm{cl} : P(G) \to P(G)$ uma função (em inglês, cl abrevia *closure*, fecho). G é chamado *pré-geometria* se, para todos $x, y \in G$ e $X, Y \subseteq G$,

(i) $X \subseteq \text{cl}(X)$ e se $X \subseteq \text{cl}(Y)$ então $\text{cl}(X) \subseteq \text{cl}(Y)$.

(ii) Se $x \in \text{cl}(X)$ então existe um subconjunto finito X_0 de X de modo que $x \in \text{cl}(X_0)$.

(iii) Se $x \in \text{cl}(X \cup \{y\})$, mas $x \notin \text{cl}(X)$, então $y \in \text{cl}(X \cup \{x\})$, propriedade conhecida como *(MacLane–)Steinitz exchange axiom.*

O conjunto $\text{cl}(X)$ é o *fecho* de X e os conjuntos $X = \text{cl}(X)$ são ditos *fechados*.

G é chamado *geometria* se ainda $\text{cl}(\emptyset) = \emptyset$ e $\text{cl}(\{x\}) = \{x\}$ para todo $x \in G$.

Um *isomorfismo* entre pré-geometrias G, H é uma bijeção $f : G \to H$ tal que sempre $f[\text{cl}_G(X)] = \text{cl}_H(f[X])$.

Essa definição é afinada para uso modelo-teórico: a propriedade (ii) é diferentemente formulada para diferentes aplicações. O texto de Crapo e Rota adota $\text{cl}(X_0) = \text{cl}(X)$ na página 2.4 e o texto de Welsh trabalha apenas com conjuntos finitos, conforme seu Teorema 1.2.4.

Fato 3.3.2. $\text{cl}(\text{cl}(X)) = \text{cl}(X)$ e $X \subseteq Y$ implica $\text{cl}(X) \subseteq \text{cl}(Y)$.

Temos $\text{cl}(X) \subseteq \text{cl}(X) \Rightarrow \text{cl}(\text{cl}(X)) \subseteq \text{cl}(X) \subseteq \text{cl}(\text{cl}(X))$ e $X \subseteq Y \subseteq \text{cl}(Y) \Rightarrow \text{cl}(X) \subseteq \text{cl}(Y)$.

Facilmente se verificam os axiomas para a geometria em que todos os conjuntos são fechados: $\text{cl}(X) = X$.

Um espaço vetorial é uma pré-geometria com $\text{cl}(X)$ o subespaço gerado por X. Nesse caso, $\text{cl}(X)$ é o conjunto das combinações lineares (finitas) de elementos de X, de modo que por definição satisfazem-se as condições (i) e (ii). Para verificar (iii), lembramos que se $x \in \text{cl}(X \cup \{y\})$, mas $x \notin \text{cl}(X)$, então y ocorre na combinação linear que iguala x com um coeficiente não-nulo; fatorando, obtemos y como combinação linear de x e dos mesmos elementos de X. Contudo, o espaço não é uma geometria porque $\text{cl}(\emptyset) = \{0\}$. Veremos que algumas definições e propriedades de pré-geometria são apenas generalizações daquelas válidas em espaços vetoriais.

Exemplo 3.3.3. Um corpo K é uma pré-geometria com $\text{cl}(X)$ o fecho algébrico (tradicional de Álgebra) em K do subcorpo gerado por X, ou seja, $\text{cl}(X)$ é o conjunto das raízes dos polinômios não-nulos com coeficientes no subcorpo gerado por X. Na linguagem dos anéis com unidade, os elementos desse subcorpo são quocientes de elementos obtidos de X por termos também polinomiais.

A propriedade (i) é usual em Álgebra. Para (ii), lembramos o raciocínio de que o polinômio e os termos são finitos, de modo que apenas um número finito de elementos de X são necessários para escrever um polinômio.

Quanto a (iii), suponha $x \in \mathrm{cl}(X \cup \{y\})$ e $x \notin \mathrm{cl}(X)$. Desse modo, y precisa ocorrer nos termos dos coeficientes do polinômio com raiz x. Multiplicando pelo produto dos denumeradores, y é raiz de polinômio com termos polinomiais. Como os termos correspondem a polinômios, por fatoração obtemos um polinômio com raiz y e coeficientes obtidos de $X \cup \{x\}$ por termos. Então $y \in \mathrm{cl}(X \cup \{x\})$.

Há também outras duas geometrias muito importantes baseadas em espaços vetoriais:

Exemplo 3.3.4 (Geometria afim). Suponha que V é um espaço vetorial. Um *espaço afim* é um transladado de um subespaço vetorial, ou seja, $a + W$. Tome G o conjunto de pontos de V. O fecho de um conjunto $X \subseteq G$ é o menor espaço afim de V contendo X. Verifica-se que G é uma geometria: como existem espaços afins disjuntos por translação, $\mathrm{cl}(\emptyset) = \emptyset$. Note que a situação é semelhante à da original de espaços vetoriais, porém aqui a origem 0 perde sua relevância.

Exemplo 3.3.5 (Geometria projetiva). Suponha que V é um espaço vetorial. Tome G o conjunto de retas de V contendo a origem, ou seja, G é o conjunto dos subespaços vetoriais de V gerados por um único vetor não-nulo. O fecho de um conjunto $X \subseteq G$ é a menor família dessas retas que contém X e está contida em um subespaço de V. Verifica-se que G é uma geometria.

Definição 3.3.6. Suponha $A \subseteq X \subseteq G$.

Diz-se que A *gera* X se $X \subseteq \mathrm{cl}(A)$, ou seja, $\mathrm{cl}(A) = \mathrm{cl}(X)$.

Diz-se que A é *independente* se, para todo $a \in A$, $a \notin \mathrm{cl}(A - \{a\})$.

Se A gera X e é independente, A é chamado *base* de X.

Por exemplo, a base usual em um espaço vetorial. (Veja também o Exemplo 3.3.9.) Algumas propriedades de conjuntos geradores ou (linearmente) independentes de espaços vetoriais generalizam-se, com as mesmas demonstrações, para pré-geometrias. Contentar-nos-emos em estudar a

Proposição 3.3.7. Todo $X \subseteq G$ contém um conjunto independente maximal, que é uma base de X, contendo um subconjunto independente dado. Todas as suas bases tem a mesma cardinalidade, indicada $\dim X$ e chamada *dimensão* de X.

Referências: O Lema 6.1.9 de [Marker] ou os Teoremas 1 e 2 da Seção III.5 de [Lang]. Revisemos o roteiro usual da demonstração para espaços vetoriais: a existência do conjunto independente maximal; o fato de ser gerador; a invariância da cardinalidade.

Dado um subconjunto independente de X, por exemplo $\emptyset$, aplicamos o Lema de Zorn para concluir que X tem um subconjunto independente maximal A. Isso envolve mostrar que é independente a união de qualquer cadeia de conjuntos independentes, momento em que a propriedade (ii) da definição de pré-geometrias permite estudar uma subcadeia finita.

A condição (iii) implica que A gera X, porque se x não fosse gerado obteríamos $A \cup \{x\}$ independente, contradizendo a maximalidade de A.

Novo uso das propriedades definidoras mostra que duas bases finitas têm o mesmo número de elementos: o número constante de geradores necessários da união de ambas. Finalmente, a condição (ii) generaliza o resultado para bases infinitas.

O Exemplo 3 da pág. 167 e o "Primeiro alerta" da pág. 172 de [Hodges] avisam que a dimensão geométrica das geometrias afins e projetivas é 1 a menos que a dada pela proposição, baseada em números de pontos necessários para determinar o conjunto. Por exemplo, uma reta tem dimensão geométrica 1, como aprendemos mesmo intuitivamente, mas dimensão 2 porque é determinada por dois pontos seus.

Generalizamos, agora, a construção do quociente de espaços vetoriais. Se V é um tal espaço e H um seu subespaço, temos $a + H = b + H \Leftrightarrow a - b \in H \Leftrightarrow a \in \mathrm{cl}(\{b\} \cup H)$.

Proposição 3.3.8. Sejam G uma pré-geometria e $S \subseteq G$. A aplicação $\mathrm{cl}_S : P(G) \to P(G)$, $\mathrm{cl}_S(X) = \mathrm{cl}(X \cup S)$, é chamada *localização* e transforma o conjunto G em uma nova pré-geometria indicada G/S. Para $S \subseteq Y \subseteq G$, temos $\dim_G Y = \dim_G S + \dim_{G/S} Y$.

Demonstração: Verificaremos apenas a equação das dimensões, sendo as propriedades de pré-geometria diretamente válidas. Suponha B uma base de S, de modo que $B \subseteq S$, $S \subseteq \mathrm{cl}(B)$ e B é independente em G também, por definição. B estende-se a uma base C de Y. Tome $A = C - B$, de modo que $|C| = |B| + |A|$. Então $C \subseteq (C - B) \cup S = A \cup S \subseteq Y$, donde $Y = \mathrm{cl}(C) \subseteq \mathrm{cl}(A \cup S)$ e $A \cup S$ gera Y, ou seja, A gera Y em G/S. Dado $a \in A$, temos $a \in C$ e $a \notin \mathrm{cl}(C - \{a\})$. Como $B \subseteq C - \{a\}$, vem $S \subseteq \mathrm{cl}(C - \{a\})$ e $(C - \{a\}) \cup S \subseteq \mathrm{cl}(C - \{a\})$, donde $a \notin \mathrm{cl}((C - \{a\}) \cup S) \supseteq \mathrm{cl}_S(A - \{a\})$. Desse modo, A é base de Y em G/S.

QED

Parafraseemos a independência em pré-geometrias obtidas por localização: Y é independente sobre X, ou os elementos de Y o são sobre X, se para todo $y \in Y$ temos $y \notin \mathrm{cl}_X(Y - \{y\}) = \mathrm{cl}(X \cup (Y - \{y\}))$.

Indicaremos a dimensão de qualquer conjunto Y sobre X também como $\dim(Y/X)$, mesmo que Y não contenha X.

Exemplo 3.3.9. Suponha $K \subseteq L$ corpos e $X \subseteq L$. Podemos tomar uma base de transcendência $X_0 \subseteq X$ de $K(X)$ sobre K, de modo que $K(X)$ é extensão algébrica de $K(X_0)$. Então $K(X) \subseteq \mathrm{cl}(K(X_0)) = \mathrm{cl}(K \cup X_0) = \mathrm{cl}_K(X_0)$ (porque $K \cup X_0$ gera o subcorpo $K(X_0)$). Dado $x \in X_0$, sabemos que $x \notin \mathrm{cl}(K \cup (X_0 - \{x\}))$. Então X_0 é base de $K(X)$ sobre K e $\dim(K(X)/K) = |X_0|$ igual ao grau de transcendência de $K(X)$ sobre K. Note que também $\dim(X/K) = |X_0|$ porque $X \subseteq K(X)$.

Em particular, $\dim(L/K)$ é o grau de transcendência de L sobre K e $\dim(K)$ é o grau de transcendência de K sobre seu corpo primo.

Definição 3.3.10. Suponha G uma pré-geometria.

(i) Se para todos $X, Y \subseteq G$ fechados de dimensão finita vale

$$\dim X + \dim Y = \dim(X \cup Y) + \dim(X \cap Y) ,$$

então dizemos que G é *modular*. (Sabe-se que a equação já vale quando X ou Y tem dimensão infinita.)

(ii) Diz-se que G é *localmente modular* se existe $a \in G$ tal que a localização de G em $\{a\}$ seja modular.

(iii) Diz-se que G é *trivial ou degenerada* se $\mathrm{cl}(X) = \bigcup_{x \in X} \mathrm{cl}(\{x\})$ para todo $X \subseteq G$.

Exemplo 3.3.11. Um corpo algebricamente fechado K de grau de transcendência infinito sobre seu corpo primo K_0 ***não*** é localmente modular. Suponha $a, b, x \in K$ algebricamente independentes sobre K_0. Tome $y = ax + b$. Então $\dim(K_0(x, y, a, b)/K_0) = 3$ e $\dim(K_0(x, y)/K_0) = \dim(K_0(a, b)/K_0) = 2$, mas $K_0(x, y) \cap K_0(a, b) = K_0$.

Espaços vetoriais são modulares, mas geometrias afins não, porque existem retas "paralelas". Estas geometrias são apenas localmente modulares.

Apresentamos, neste fato, uma construção de que não faremos uso, para conveniência do leitor que consultar nossas referências sobre a Conjectura de Zilber.

Fato 3.3.12. Dada uma pré-geometria G, tome G' o conjunto dos fechos $\mathrm{cl}(\{x\})$ de $x \in G - \mathrm{cl}(\emptyset)$ e defina, para $X' \subseteq G'$, seu fecho $\mathrm{cl}'(X') = \{\mathrm{cl}(\{x\}) \in G' \mid x \in \mathrm{cl}(\bigcup X')\}$. Então G' é uma geometria, dita *(canonicamente) associada a G*.

Equivalentemente, pode-se definir em $G_0 = G - \mathrm{cl}(\emptyset)$ a relação de equivalência $x \sim y \Leftrightarrow \mathrm{cl}(\{x\}) = \mathrm{cl}(\{y\})$. Tome G' o conjunto das classes de equivalência de $\sim$ e defina, para $X' \subseteq G'$, seu fecho $\mathrm{cl}'(X')$ como o conjunto das classes $(x/\sim) \in G'$ dos elementos $x \in \mathrm{cl}(\{y \in G \mid (y/\sim) \in X'\})$.

Todo automorfismo de G induz naturalmente um automorfismo de G'.

Em espaços vetoriais, G' corresponde ao conjunto de retas pela origem de G, ou seja, é a geometria projetiva.

3.4. Conjuntos fortemente minimais

Sabemos que corpos algebricamente fechados são fortemente minimais e que, neles, $\mathrm{acl}(\cdot)$ é idêntico ao fecho algébrico que exploramos nos exemplos da senão anterior. Generalizaremos essa identificação, agora, em conjuntos definíveis fortemente minimais e relacionaremos a independência de pré-geometrias com a de deviação.

Fixe uma L-estrutura $\mathfrak{A}$ e um subconjunto definível $D \subseteq A$. Assumiremos que D é $\emptyset$-definível e fortemente minimal, mas enunciaremos o primeiro teorema de um modo mais geral; veremos também que admitiria prova mais simples nas condições mais fortes. Frisamos que D tem uma única "coordenada", não m como usual.

Teorema 3.4.1. Suponha que D é minimal e A_0-definível com $A_0 \subseteq A$. A aplicação que a $X \subseteq D$ associa $\mathrm{acl}(X \cup A_0) \cap D$ transforma D em uma pré-geometria.

Demonstração: Já estudamos as duas primeiras condições da definição de pré-geometrias, de modo que nos concentraremos em verificar o *Steinitz exchange axiom*. Suponha $X \subseteq D$ e $a, b \in D$. Seja $\delta(v)$ a fórmula de $\mathrm{L}(A_0)$ que define D. Todas as fórmulas a seguir serão de $\mathrm{L}(XA_0)$. Suponha $a \in \mathrm{acl}(XA_0b)$, mas $a \notin \mathrm{acl}(XA_0)$.

Existe uma fórmula $\phi(v, w)$ de modo que $a \in \phi(\mathfrak{A}, b)$ finito. Sejam $n = |D \cap \phi(\mathfrak{A}, b)| = |\{d \in D | \mathfrak{A} \models \phi(d, b)\}|$ e $\psi(w) : \exists^{=n} v\,(\delta(v) \wedge \phi(v, w))$. Então $\mathfrak{A} \models \psi(b)$. Se ψ definisse um conjunto finito, então $b \in \mathrm{acl}(XA_0)$ e de $XA_0b \subseteq \mathrm{acl}(XA_0)$ concluiríamos que $\mathrm{acl}(XA_0b) \subseteq \mathrm{acl}(\mathrm{acl}(XA_0)) = \mathrm{acl}(XA_0)$, contradição. Por D ser minimal, ψ define um conjunto cofinito em D.

Se $\{d \in D \mid \mathfrak{A} \models \phi(a, d) \wedge \psi(d)\}$ é finito, por conter b temos $b \in \mathrm{acl}(XA_0a)$ como desejado (fórmula $\delta(w) \wedge \phi(a, w) \wedge \psi(w)$). Mostremos que a outra possibilidade, ser cofinito em D, é absurda. Suponha que seu complemento em D tem cardinalidade k. Seja $\chi(v) : \exists^{=k} w\,(\delta(w) \wedge \neg(\phi(v, w) \wedge \psi(w)))$. Temos $\mathfrak{A} \models \chi(a)$. Se χ define um conjunto finito, obtemos $a \in \mathrm{acl}(XA_0)$, absurdo. Se χ define um cofinito em D, como este é infinito contém $a_1, \ldots, a_{n+1}$ distintos satisfazendo χ. Para cada i, o conjunto $D_i = \{d \in D \mid \mathfrak{A} \models \phi(a_i, d) \wedge \psi(d)\}$ é cofinito em D, por $\mathfrak{A} \models \chi(a_i)$. A intersecção $\bigcap_{i=1}^{n+1} D_i$ é, portanto, não-vazia (D infinito), contendo um elemento d_0. Então $\mathfrak{A} \models \phi(a_1, d_0), \ldots, \phi(a_{n+1}, d_0)$, de modo que $|\{d \in D \mid \mathfrak{A} \models \phi(d, d_0)\}| \geqslant n+1$, contradizendo $\mathfrak{A} \models \psi(d_0)$. QED

Novamente, é importante rever o conceito de independência. Suponha, no enunciado, $A_0 = \emptyset$. Para $x \in D$ e $X, Y \subseteq D$, x independe de Y sobre X se $x \notin \operatorname{acl}(X \cup Y)$ (não é preciso intersectar com D porque $x \in D$). Também para $a_1, \ldots, a_k \in D$ e $X \subseteq D$, os elementos $a_1, \ldots, a_k$ são independentes sobre X se, para todo i, $a_i \notin \operatorname{acl}(\{a_j\}_{j \neq i} \cup X)$. Essas são as formulações com que mais trabalharemos. *Note que podem **não** existir seqüências de elementos independentes, como no caso $D = X = A$.*

Impomos agora que D seja $\emptyset$-definível e fortemente minimal. Consideraremos por toda a seção o fecho $\operatorname{acl}(\cdot) \cap D$, o que implica assumir $X \subseteq D$ para trabalhar com os conceitos da seção anterior. *Desse modo, trabalharemos nas pré-geometrias D e D/X.*

Teorema 3.4.2. Se $x \in D$ e $X, Y \subseteq D$, então $x \in \operatorname{acl}(X \cup Y) - \operatorname{acl}(X)$ se e somente se $x \not\perp_X Y$. Desse modo, para $x \notin \operatorname{acl}(X)$, o conceito "$x$ independe de Y sobre X" é o mesmo formulado geometricamente ou com deviação.

Demonstração: Note que $D \in t(x/X)$ e $\operatorname{RM}(x/X) \leqslant \operatorname{RM}(D) \leqslant 1$.

Se $x \in \operatorname{acl}(XY)$ então $t(x/XY)$ tem posto 0; se $x \notin \operatorname{acl}(X)$ então $t(x/X)$ tem posto 1. Desse modo, $t(x/XY)$ desvia-se sobre X.

Se $t(x/XY)$ desvia-se sobre X então $0 \leqslant \operatorname{RM}(x/XY) < \operatorname{RM}(x/X) \leqslant 1$. Concluímos que de fato $t(x/XY)$ tem posto 0 e $t(x/X)$ tem posto 1, e $x \in \operatorname{acl}(XY) - \operatorname{acl}(X)$. QED

Observamos que este resultado permite provar o anterior no caso particular de D ser $\emptyset$-definível e fortemente minimal: se $a \in \operatorname{acl}(Xb) - \operatorname{acl}(X)$ então $a \not\perp_X b$ e, por simetria, $b \not\perp_X a$, donde $b \in \operatorname{acl}(Xa) - \operatorname{acl}(X)$.

Lema 3.4.3. É único o m-tipo sobre X das m-uplas de D independentes sobre X. Veremos no Corolário 3.4.5 que esse tipo também é exclusivo de tais m-uplas.

Demonstração: Sejam $a_1, \ldots, a_m, b_1, \ldots, b_m \in D$ com a_i independentes sobre X e b_i também. O enunciado afirma que $t(a_1, \ldots, a_m/X) = t(b_1, \ldots, b_m/X)$. Procederemos por indução em m.

Se $m = 1$, então $a_1, b_1 \notin \operatorname{acl}(X)$. Sendo E um X-definível qualquer, temos $a_1 \in E$ se e somente se $D \cap E$ é infinito, porque D é minimal e a_1 não pertence a X-definíveis finitos. O mesmo vale para b_1, de modo que $a_1 \in E \Leftrightarrow b_1 \in E$, ou seja, $t(a_1/X) = t(b_1/X)$.

Suponha agora que $m > 1$ e que o enunciado valha para $m-1$ e escreva θ a fórmula de $\mathrm{L}(X)$ que define D.

Retirando-se a_m e b_m, mantém-se a hipótese de independência e $t(a_1, \ldots, a_{m-1}/X) = t(b_1, \ldots, b_{m-1}/X)$. Seja ϕ uma fórmula de $\mathrm{L}(X)$ com m variáveis livres, tal que $\mathfrak{A} \models \phi(a_1, \ldots, a_m)$. Como $a_m \notin \mathrm{acl}(X \cup \{a_1, \ldots, a_{m-1}\})$, $a_m \in D \cap \phi(a_1, \ldots, a_{m-1}, \mathfrak{A})$ e D é minimal, obtemos $D - \phi(a_1, \ldots, a_{m-1}, \mathfrak{A})$ finito, digamos com k elementos. Então $\mathfrak{A} \models \exists^{=k} v\, (\theta(v) \wedge \neg\phi(a_1, \ldots, a_{m-1}, v))$, de modo que

$$\exists^{=k} v\, (\theta(v) \wedge \neg\phi(v_1, \ldots, v_{m-1})(v)) \in t(a_1, \ldots, a_{m-1}/X)\,.$$

Pela igualdade dos tipos, obtemos $\mathfrak{A} \models \exists^{=k} v\, (\theta(v) \wedge \neg\phi(b_1, \ldots, b_{m-1}, v))$, de modo que $D - \phi(b_1, \ldots, b_{m-1}, \mathfrak{A})$ tem k elementos e $D \cap \phi(b_1, \ldots, b_{m-1}, \mathfrak{A})$ é infinito. Como $b_m \notin \mathrm{acl}(X \cup \{b_1, \ldots, b_{m-1}\})$ e D é minimal, obtemos $b_m \in D \cap \phi(b_1, \ldots, b_{m-1}, \mathfrak{A})$ e $\mathfrak{A} \models \phi(b_1, \ldots, b_m)$. Concluímos assim que se ϕ pertence a $t(a_1, \ldots, a_m/X)$ então pertence também a $t(b_1, \ldots, b_m/X)$. Um tipo está contido no outro e obtemos a igualdade desejada. QED

Teorema 3.4.4. $\mathrm{RM}(a_1, \ldots, a_m/X) = \dim(\{a_1, \ldots, a_m\}/X)$ para quaisquer $a_1, \ldots, a_m \in D$ e $X \subseteq D$.

Demonstração: Mostraremos que, se $a_1, \ldots, a_m \in D$ são independentes sobre X, então $\mathrm{RM}(a_1, \ldots, a_m/X) = m$. O caso geral do enunciado segue então pela Proposição 3.2.1, para índices $\geqslant m$, bastando considerar uma base de $\{a_1, \ldots, a_{m+k}\}$ sobre X.

Prossigamos por indução na dimensão m. Para $m = 1$, temos $D \in t(a_1/X)$, de modo que esse tipo tem posto 0 ou 1. Se tem posto 0, então $a_1 \in \mathrm{acl}(X)$ e $\dim(\{a_1\}/X) = 0$. Se tem posto 1, então $a_1 \notin \mathrm{acl}(X)$ e $\dim(\{a_1\}/X) = 1$, porque $\{a_1\}$ é base.

Suponha então $m \geqslant 2$ e que o caso particular valha até $m-1$. Primeiramente, computemos $\dim(\{a_2, \ldots, a_m\}/Xa_1) = m-1$. Sobre Xa_1, o conjunto $\{a_2, \ldots, a_m\}$ é independente porque, para todo $i \geqslant 2$,

$$a_i \notin \mathrm{acl}(\{a_j\}_{j \neq i} \cup X) = \mathrm{acl}(\{a_j\}_{j \neq 1, i} \cup Xa_1)\,.$$

Pela Proposição 3.2.1 aplicada a Xa_1 e pela hipótese de indução, temos $\mathrm{RM}(a_1, \ldots, a_m/Xa_1) = \mathrm{RM}(a_2, \ldots, a_m/Xa_1) = \dim(\{a_2, \ldots, a_m\}/Xa_1) = m-1$.

Por independência, porém, $a_1 \in \mathrm{acl}(Xa_1 \ldots a_m) - \mathrm{acl}(Xa_2 \ldots a_m)$, ou melhor ainda, $a_1 \in \mathrm{acl}(Xa_1 \ldots a_m) - \mathrm{acl}(X)$. Assim, $a_1 \not\mathrel{\perp\!\!\!\perp}_X \{a_1, \ldots, a_m\}$. Por simetria, $(a_1, \ldots, a_m) \not\mathrel{\perp\!\!\!\perp}_X a_1$ e então $\mathrm{RM}(a_1, \ldots, a_m/X) > \mathrm{RM}(a_1, \ldots, a_m/Xa_1) = m-1$.

Para agora mostrar que é impossível $\mathrm{RM}(a_1, \dots, a_m/X) > m$, tomaremos $\mathfrak{B}$ uma extensão elementar ω-saturada de $\mathfrak{A}$ e $\mathfrak{C}$ uma extensão elementar $|B|^+$-saturada de $\mathfrak{B}$. Seja $D(\mathfrak{B})$ o conjunto definido em $\mathfrak{B}$ pela fórmula que define D.

Suponha que $(a_1, \dots, a_m) \in E \in \mathrm{Def}^m_{\mathfrak{B},X}$, ou seja, E pertence ao tipo de $(a_1, \dots, a_m)$. Podemos supor que $E \subseteq (D(\mathfrak{B}))^m$, porque este é um $\emptyset$-definível com o qual podemos intersectar E, lembrando que cada $a_i \in D(\mathfrak{B})$. Assumindo que $\mathrm{RM}(a_1, \dots, a_m/X) > m$, obtemos $\mathrm{RM}(E) \geqslant m + 1$.

Como $\mathfrak{B}$ é ω-saturada, pelo Lema 2.1.10 existem $E_1, E_2 \in \mathrm{Def}^m_{\mathfrak{B},B}$ de posto m contidos em E e disjuntos. Sejam $D(\mathfrak{C}), E_1(\mathfrak{C}), E_2(\mathfrak{C})$ os definíveis correspondentes em $\mathfrak{C}$. Porque todos os tipos sobre B são realizados em $\mathfrak{C}$, existem $e_i \in E_i(\mathfrak{C})$ com $\mathrm{RM}(e_i/B) = m$. Mas $t(e_1/B) \neq t(e_2/B)$ porque $E_1 \cap E_2 = \emptyset$, de modo que, em vista do Lema 3.4.3, um desses tipos ***não*** é o tipo das m-uplas de $D(\mathfrak{C})$ independentes sobre B, caso exista. (Lembramos que também $D(\mathfrak{C})$ é fortemente minimal e, no lema, a hipótese $B \subseteq D(\mathfrak{C})$ é necessária somente para uso da terminologia.)

Suponha que $t(e_1/B)$ satisfaz esse quesito. Escreva $e_1 = (c_1, \dots, c_m) \in C^m$ e, reordenando os índices para conveniência, $c_m \in \mathrm{acl}(Bc_1 \dots c_{m-1})$. Seja θ a fórmula de $\mathrm{L}(B)$ tal que $\mathfrak{C} \models \theta(c_1, \dots, c_m), \exists^{\leqslant k} v\, \theta(c_1, \dots, c_{m-1}, v)$, com $k \in \mathbb{N}$. Tome ϕ a conjunção da fórmula que define E_1 e θ e $\exists^{\leqslant k} v\, \theta(v_1, \dots, v_{m-1}, v)$, todas nas variáveis $v_1, \dots, v_m$.

Como $\phi(\mathfrak{C})$ é um B-definível não-vazio e contido em $E_1(\mathfrak{C})$ com posto, esse conjunto determina um tipo $t(d/B)$, em que $d \in C^m$ porque os tipos sobre B são realizados em $\mathfrak{C}$. Temos $d \in E_1(\mathfrak{C})$ e $d_m \in \mathrm{acl}(Bd_1 \dots d_{m-1})$. Observe, finalmente, que $d \in D(\mathfrak{C})^m$.

Assim, $\dim(d/B) \leqslant m - 1 < m$. Por hipótese de indução, $\mathrm{RM}(\phi(\mathfrak{C})) = \mathrm{RM}(d/B) \leqslant m - 1 < m$. Contudo, $e_1 \in \phi(\mathfrak{C})$, de modo que $\phi(\mathfrak{C}) \in t(e_1/B)$ e $m = \mathrm{RM}(e_1/B) \leqslant \mathrm{RM}(\phi(\mathfrak{C}))$, contradição. QED

Corolário 3.4.5. Se existirem m-uplas de D independentes sobre X, qualquer m-upla de D que satisfizer seu tipo sobre X também é independente.

Demonstração: Existindo m-uplas independentes, seu tipo tem posto m e qualquer m-upla que o satisfaça será um conjunto de dimensão m, portanto independente. QED

Corolário 3.4.6. Para cada fórmula $\phi(v_1, \dots, v_n, w)$ de L que implique que os elementos que realizem $v_1, \dots, v_n$ pertencem a D e para cada $k \in \mathbb{N}$, o conjunto $\{b \in D \mid \mathrm{RM}(\phi(\mathfrak{A}, b)) = k\}$ é definível.

Referências: O Corolário 5.6 de [Ziegler] ou o Lema 6.2.20 de [Marker].

Exemplo 3.4.7. Suponha $K \subseteq L$ corpos e L algebricamente fechado. Então $\mathrm{acl}(\cdot)$ é o fecho algébrico tradicional e L é $\emptyset$-definível fortemente minimal. Se $a_1, \ldots, a_n \in L$, temos $\mathrm{RM}(a_1, \ldots, a_n/K) = \dim(\{a_1, \ldots, a_n\}/K) = \dim(K(a_1, \ldots, a_n)/K)$ igual ao grau de transcendência dessa extensão pelo Exemplo 3.3.9.

Corolário 3.4.8 (Equação de Lascar). Para todas as seqüências não-vazias a, b em D e $X \subseteq D$, vale $\mathrm{RM}(a, b/X) = \mathrm{RM}(a/Xb) + \mathrm{RM}(b/X)$.

Demonstração: Tome S o conjunto dos elementos de b, ou $S = b$, e Y o conjunto dos elementos de a e b, ou $Y = ab$. Pela Proposição 3.3.8, $\dim_{D/X} Y = \dim_{D/X} S + \dim_{(D/X)/S} Y$. O operador fecho em D/X, porém, é dado por $\mathrm{cl}_X(Z) = \mathrm{acl}(Z \cup X)$; em $(D/X)/S$ é dado por $\mathrm{cl}_S(Z) = \mathrm{cl}_X(Z \cup S) = \mathrm{acl}(Z \cup (X \cup S))$. Assim, $\dim_{(D/X)/S} Y = \dim_{D/X \cup S} Y$ e obtemos $\dim(ab/X) = \dim(b/X) + \dim(ab/Xb)$.

Pelo teorema anterior, $\mathrm{RM}(a, b/X) = \mathrm{RM}(b/X) + \mathrm{RM}(ab/Xb)$. Contudo, cada elemento de b pertence a $\mathrm{acl}(Xb) \subseteq \mathrm{acl}(Xba)$ e, pela Proposição 3.2.1, $\mathrm{RM}(ab/Xb) = \mathrm{RM}(a/Xb)$.

Note que aqui, como os postos são dimensões finitas ($|Y| < \omega$), a soma comuta. QED

Concluímos com a

Proposição 3.4.9. Suponha X um fechado de D e $a, b \in D - X$. Então existe um automorfismo da pré-geometria de D que fixa os elementos de X e leva a a b. Diz-se que a pré-geometria é *homogênea*.

Demonstração: Apresentaremos uma prova completa para o caso particular em que $\mathfrak{A}$ é fortemente $|X|^+$-homogênea e comentaremos como o caso geral é apresentado em [Hodges].

Cada um de a e b é um elemento independente de X, porque $a, b \notin \mathrm{acl}(X) \cap D = X$. Assim, $t(a/X) = t(b/X)$ e, sob a hipótese de homogeneidade forte, existe um automorfismo σ de $\mathfrak{A}$ sobre X com $\sigma(a) = b$. Como D é $\emptyset$-definível, temos $\sigma[D] = D$. Se $Y \subseteq D$, considere uma fórmula com parâmetros em Y: porque σ é elementar, obtemos $\sigma[\mathrm{acl}(Y) \cap D] = \mathrm{acl}(\sigma[Y]) \cap D$. Concluímos que $\sigma|_D$ é um automorfismo da pré-geometria D.

Em geral, [Hodges] deriva a mesma conclusão de dois resultados seus.

Primeiramente, lembre que, porque $t(a/X) = t(b/X)$, a função que fixa cada elemento de X e leva a a b é uma função (parcial) elementar. Se Xa e Xb são estendidos a bases de D, os elementos adicionais podem ser postos em correspondência biunívoca e indexados por um ordinal; do mesmo modo, por indução transfinita se conclui que a bijeção entre as duas bases é uma função elementar. Esse é um caso particular de seu Lema 4.5.6.

Seu Lema 4.5.5, adaptado, aplica o Lema de Zorn para estender essa bijeção a uma função parcial elementar com domínio e imagem iguais a D. Porque é elementar, essa bijeção é um automorfismo da pré-geometria D. QED

Espaços vetoriais são homogêneos, porque podemos estender uma base do fechado a bases do espaço, cada uma contendo um dos pontos, e bijeções entre bases geram automorfimos. Também corpos algebricamente fechados são homogêneos, como observamos na Seção 1.2.

Retomaremos o estudo da pré-geometria de um $\emptyset$-definível fortemente minimal na Seção 4.2.

3.5. Ortogonalidade

Este material é conteúdo da Seção 6 de [Ziegler] e usa o fecho $\mathrm{acl}^{\mathrm{eq}}(\cdot)$, que apresentaremos no próximo capítulo; o leitor pode postergar sua leitura. Assumimos agora que T é uma teoria ω-estável e $\mathfrak{C}$ é um modelo monstro de T, com cardinalidade de saturação ou grandeza a ser especificada. Denotamos $D, E \in \mathrm{Def}^1_C$.

Definição 3.5.1. Os definíveis D, E são *ortogonais* e indica-se $D \perp E$ se quaisquer dois elementos $d \in D$ e $e \in E$ são independentes sobre qualquer conjunto de parâmetros sobre o qual D e E possam ser definidos.

As propriedades de deviação implicam que, se de e $Y \supseteq X$ são independentes sobre X, então $d \downarrow_X e \Leftrightarrow d \downarrow_Y e$. Desse modo, ortogonalidade falha para toda extensão Y se falha para o conjunto de parâmetros X.

Esta caracterização não menciona deviação:

Lema 3.5.2. D, E são ortogonais se e somente se, para todos $d, e \in C$, $d_0 \in D$ e $e_0 \in E$ e todo conjunto X sobre o qual D e E são definíveis, com $X = \mathrm{acl}^{\mathrm{eq}}(X)$, $t(d/X) = t(d_0/X)$ e $t(e/X) = t(e_0/X)$, vale $t(de/X) = t(d_0e_0/X)$.

Demonstração: A condição significa que $t(d/X)$ tem uma única extensão a um tipo sobre Xe, notadamente $t(d/Xe)$, que portanto deve ser a extensão direta. Isso implica que todos d, e são independentes sobre todos os conjuntos fechados por $\mathrm{acl}^{\mathrm{eq}}(\cdot)$, o que basta para $D \perp E$. Reciprocamente, ortogonalidade implica que $t(d/X)$ tem apenas extensões indivisíveis a Xe, que são uma única se X é $\mathrm{acl}^{\mathrm{eq}}$-fechado. QED

Lema 3.5.3. Um definível D fortemente minimal não é ortogonal ao um definível E se e somente se $D \subseteq \mathrm{acl}(X \cup E)$ para algum conjunto finito de parâmetros X.

Demonstração: Para a implicação direta, suponha $D \subseteq \operatorname{acl}(X \cup E)$. Escolha $d \in D - \operatorname{acl}(X)$ e um subconjunto minimal $\{e_1, \ldots, e_n\} \subseteq E$ tal que $d \in \operatorname{acl}(X \cup \{e_1, \ldots, e_n\})$. Então $d \not\perp_{X \cup \{e_1, \ldots, e_{n-1}\}} e_n$. Para a recíproca, $d \not\perp_X e$ para algum X sobre o qual D e E são definíveis implica $d \in \operatorname{acl}(Xe) - \operatorname{acl}(X)$. Já que todos $d' \in D - \operatorname{acl}(X)$ têm o mesmo tipo sobre X temos $D - \operatorname{acl}(X) \subseteq \operatorname{acl}(X \cup E)$.

QED

Lema 3.5.4. Não-ortogonalidade é uma relação de equivalência para definíveis fortemente minimais.

Demonstração: Suponha D fortemente minimal não ortogonal a E, F. Se X é grande o bastante, encontramos $d_1, d_2 \in D$ e $e \in E$, $f \in F$ tais que $d_1 \in \operatorname{acl}(Xe) - \operatorname{acl}(X)$ e $d_2 \in \operatorname{acl}(Xf) - \operatorname{acl}(X)$. Já que d_1 e d_2 têm o mesmo tipo sobre X podemos assumir $d_1 = d_2$, donde $d_1 \not\perp_X d_2$, o que implica $e \not\perp_X f$. Isso mostra que E não é ortogonal a F. QED

O restante da Seção 6 de [Ziegler] aplica-se à teoria de grupos que estudaremos no Capítulo 5.

4
Interpretações

Explicitaremos a mais importante definição de nosso texto, que dá significado preciso a "interpretar uma estrutura em outra". Essa noção é antiga na teoria e pode ser encontrada mesmo antes, por exemplo na construção de modelos da Geometria Hiperbólica no espaço euclideano. Embora só a utilizemos em algumas situações, serão todas intimamente relacionadas a nosso objetivo final.

Também construiremos a estrutura $\mathfrak{A}^{\mathrm{eq}}$ devida a Shelah, que permite tratar as interpretações em uma linguagem "uniforme". Embora essa construção não seja essencial à teoria, é usada em muitos textos, tornando-se mesmo um pré-requesito vocabular.

Por exemplo, uma caracterização modelo-teórica de famílias de curvas planas fundamenta-se em bases canônicas, e a Conjectura de Zilber descreve as interpretações não-triviais.

Trabalharemos com uma linguagem L arbitrária.

4.1. O conceito

Apresentaremos a formulação usada em [Marker] e [Poizat 1], embora neste texto "definível" seja sinônimo de "interpretável". Para propósitos mais diversos, esta definição pode ser generalizada sintática ou semanticamente, como em [Hodges]. Logo em seguida, apresentamos uma formulação equivalente, em termos de definíveis, usada por exemplo em [Hrushovski, Zilber].

Definição 4.1.1. Suponha L_0, L duas linguagens arbitrárias e $\mathfrak{A}_0$ uma L_0-estrutura e $\mathfrak{A}$ uma L-estrutura.

Suponha $U \in \mathrm{Def}^n_{\mathfrak{A},\emptyset}$, um subconjunto $\emptyset$-definível de U^k para cada predicado k-ário de L_0, uma função $\emptyset$-definível de U^k a U para cada operador k-ário de L_0 e um elemento $\emptyset$-definível de U para cada constante de L_0. Então, com essas interpretações, obtemos uma L_0-estrutura $(U, \ldots)$. Caso $(U, \ldots) \cong \mathfrak{A}_0$, diz-se que $\mathfrak{A}_0$ é *definível* ou *definivelmente interpretável* em $\mathfrak{A}$.

Suponha agora $U \in \mathrm{Def}^n_{\mathfrak{A},\emptyset}$ e uma relação $\emptyset$-definível de equivalência $\sim$ em U. Suponha também, como no parágrafo anterior, um $\emptyset$-definível para cada símbolo de L_0, mas que independa dos representantes das classes de equivalência de $\sim$. Então podemos, no conjunto $U/\sim$ dessas classes, interpretar cada símbolo de L_0 de modo correspondente, obtendo uma L_0-estrutura $(U/\sim, \ldots)$. Caso $(U/\sim, \ldots) \cong \mathfrak{A}_0$, diz-se que $\mathfrak{A}_0$ é *interpretável* em $\mathfrak{A}$, ou $\mathfrak{A}$ *interpreta* $\mathfrak{A}_0$.

A restrição de $\emptyset$-definibilidade é versátil para uso com teorias em vez de modelos específicos e será adequada à construção $\mathfrak{A}^{\mathrm{eq}}$, mas há situações na teoria em que se convém aceitar parâmetros.

Proposição 4.1.2. Suponha L_0, L e $\mathfrak{A}_0, \mathfrak{A}$ como na definição. $\mathfrak{A}_0$ é definível ou interpretável em $\mathfrak{A}$ se e somente se existem $n \in \mathbb{N}^*$, um $\emptyset$-definível $U \subseteq A^n$ e uma bijeção ou sobrejeção, respectivamente, $f : U \to A_0$ tal que para todo $D \in \mathrm{Def}^k_{\mathfrak{A}_0,\emptyset}$ tenhamos $f^{-1}[D] \in \mathrm{Def}^{nk}_{\mathfrak{A},\emptyset}$.

Demonstração: Estudaremos o caso interpretável–sobrejetor de modo que a situação de injeção corresponda à situação em que as classes de equivalência são unitárias. Assuma que L_0 não tem operadores nem constantes pelo Exemplo 1.1.3.

Suponha $U \subseteq A^n$ e $f : U \to A_0$ como no enunciado da proposição. Considere $\Delta = \{(x,y) \in (A_0)^2 \mid x = y\}$ a diagonal $\emptyset$-definível. Então $E = f^{-1}[\Delta] = \{(a,b) \in U^2 \mid f(a) = f(b)\}$ é, por hipótese, $\emptyset$-definível em $\mathfrak{A}$, obviamente uma relação de equivalência que denotaremos $\sim$. Cada predicado k-ário de L_0 define em $\mathfrak{A}_0$ sua interpretação correspondente $R \subseteq (A_0)^k$. Por hipótese, $f^{-1}[R]$ é $\emptyset$-definível em $\mathfrak{A}$, sendo uma relação em U^k que independe do representante de $\sim$. Obtemos a L_0-estrutura $(U/\sim, \ldots)$ isomorfa a $\mathfrak{A}_0$ pela função que leva $a/\sim$ a $f(a)$, bem-definida pela definição de $\sim$.

Suponha agora, como na definição, $(U/\sim, \ldots) \cong \mathfrak{A}_0$, sendo $\xi : (U/\sim) \to A_0$ o isomorfismo. Defina $f : U \to A_0$, $f(x) = \xi(x/\sim)$, sobrejetora. Dado $D \in \mathrm{Def}^k_{\mathfrak{A}_0,\emptyset}$, temos $\xi^{-1}[D] \in \mathrm{Def}^k_\emptyset$ em $(U/\sim, \ldots)$. Substitua, na fórmula de L_0 que define $\xi^{-1}[D]$, cada predicado pela fórmula de L que define sua interpretação em $U/\sim$. Obtemos uma fórmula de L que define $E \in \mathrm{Def}^{nk}_{\mathfrak{A},\emptyset}$, contido em U^{nk}. Para $a_1, \ldots, a_k \in U$, portanto, $(a_1, \ldots, a_k) \in E$ se e somente se $(a_1/\sim, \ldots, a_k/\sim) \in \xi^{-1}[D]$. Concluímos que $f^{-1}[D] = E$. QED

Daremos apenas um exemplo aqui — além, é claro, dos que se fizerem presentes na conclusão de nosso estudo —, convidando o leitor a buscar outros em sua área favorita da Matemática.

Exemplo 4.1.3. O corpo $\mathbb{Q}$ é interpretável no anel $\mathbb{Z}$. Tome $D = \mathbb{Z} \times \mathbb{Z}^*$, um definível de $\mathbb{Z}^2$, e a relação definível $(p,q) \sim (r,s) \Leftrightarrow ps = qr$.

Interpretam-se as relações de $\mathbb{Q}$ como ensinado para frações, sempre de modo definível. Por exemplo, $(p,q) + (r,s) = (ps + qr, qs)$, $0 = (0,1)$ e $(p,q)^{-1} = (q,p)$ se $p \neq 0$, podendo-se tomar $(0,q)^{-1} = (0,q)$.

Interpretações têm muitas propriedades interessantes, dentre as quais citamos:

Teorema 4.1.4. Suponha L_0, L e $\mathfrak{A}_0, \mathfrak{A}$ como na definição e que $\mathfrak{A}_0$ seja interpretável em $\mathfrak{A}$. Seja κ um cardinal infinito. Se $\mathfrak{A}$ é κ-saturada, então $\mathfrak{A}_0$ é κ-saturada; nesse sentido, também são induzidas κ-grandeza, κ-estabilidade, estabilidade, super-estabilidade, transcendência total e finitude do posto de Morley.

Referências: Estes resultados encontram-se dispersos em cada texto. Apresentamos apenas referências aos enunciados em [Hodges]: para κ-saturação, o Teorema 10.1.9; para κ-grandeza, o Exercício 10.4.11; para κ-estabilidade e super-estabilidade, o Exercício 6.7.15; para estabilidade, o Teorema 6.7.1(b); sobre posto de Morley, o Teorema 5.6.11.

4.2. A Conjectura de Zilber

A noção de interpretação é o último conceito necessário para enunciar uma versão da Conjectura de Zilber e comentá-la. Seguiremos a exposição comum a [Hodges], [Marker] e [Ziegler]; uma exposição alternativa é dada pelo próprio Zilber em *Dimensions and homogeneity in mathematical structures*, in A. Macintyre (ed.), *Connections between Model theory and Algebraic and Analytic Geometry*, Aracne, 2000.

Observamos que, neste texto, não trataremos da "configuração de Hrushovski (ou de Zilber ou de grupo)": o leitor interessado pode consultar a Seção 4.8 de [Hodges] ou o final da Seção 7.5 de [Marker].

Já encontramos pré-geometrias homogêneas na Proposição 3.4.9: dois pontos que não pertencem a um fechado são conjugados por um automorfismo sobre esse fechado.

Definem-se também pré-geometrias *localmente finitas*, em que o fecho de um conjunto finito sempre é finito. É o caso dos espaços vetoriais sobre corpos finitos.

Podemos então enunciar o

Teorema 4.2.1 (Cherlin–Mills–Zilber). Toda geometria G homogênea, localmente infinita e de dimensão infinita satisfaz uma destas três possibilidades:

(i) G é *desintegrada*, ou seja, todos os seus subconjuntos são fechados. (Para pré-geometrias, a condição refere-se à geometria canonicamente associada.)

(ii) G é isomorfa a uma geometria projetiva sobre um corpo finito.

(iii) G é isomorfa a uma geometria afim sobre um corpo finito.

Referência: Este é o enunciado adotado no Teorema 4.6.1 de [Hodges]. Remetemos o leitor às referências desse texto para sua Seção 4.6, na pág. 199.

Sabemos que: geometrias projetivas são modulares; geometrias afins são localmente modulares, mas não modulares; corpos algebricamente fechados de grau de transcendência infinito sobre seus corpos primos não são localmente modulares. É fácil ver que geometrias desintegradas são modulares.

Esses poucos exemplos conhecidos, à parte outros triviais, e o teorema sugeriam que todas as possibilidades já estivessem esgotadas. Em 1984, portanto, Zilber conjecturou a respeito do quê, de fato, ocorreria. Uma conseqüência, também conhecida como a própria Conjectura de Zilber, seria: "A pré-geometria de um conjunto $\emptyset$-definível fortemente minimal D com o fecho algébrico é localmente modular ou D interpreta (como domínio da interpretação) um corpo algebricamente fechado."

Hrushovski obteve um contra-exemplo para esse enunciado em 1988, mostrando que muitos dos "conjuntos fortemente minimais localmente modulares" não interpretam nem mesmo grupos. Seu raciocínio permitiu-o construir, por exemplo, uma estrutura fortemente minimal com duas estruturas de corpo (duas operações de soma e duas de produto) de características diferentes.

Para esses desenvolvimentos de Zilber e Hrushovski, remetemos o leitor às referências explicitadas em [Hodges], [Marker] e [Ziegler].

Contudo, veremos que a dicotomia entre a presença e a ausência da propriedade de modularidade local ainda é válida, como uma forma da Conjectura de Zilber, no caso de geometrias de Zariski. Estudaremos esse trabalho conjunto de Hrushovski e Zilber no Capítulo 7.

4.3. Elementos imaginários

Agora, apresentaremos a construção "eq". Adotamos a exposição comum a [Ziegler], [Pillay], [Poizat 1] e [Marker], aplicável a qualquer estrutura de qualquer linguagem.

Fixe uma L-estrutura $\mathfrak{A}$ arbitrária. Pelo Exemplo 1.1.3, podemos assumir L sem constantes ou operadores: é costume, porém, utilizar os símbolos dos operadores e constantes da linguagem original como abreviaturas informais. Sejam x, y duas seqüências de n variáveis cada.

Suponha que $\theta(x, y)$ é uma fórmula de L tal que a relação $\sim_\theta$ em A^n definida por $a \sim_\theta b \Leftrightarrow \mathfrak{A} \models \theta(a, b)$ é uma relação de equivalência em A^n. A fórmula θ é chamada *de equivalência*. A classe de equivalência de $a \in A^n$ é indicada a/θ e chamada um *elemento imaginário*. Tome $I_\theta = \{a/\theta \mid a \in A^n\}$ e $f_\theta : A^n \to I_\theta$ a projeção dada por $f_\theta(a) = a/\theta$.

(Veremos no início da demonstração da Proposição 4.3.2 como se pode considerar o caso mais geral de relação de equivalência em um *subconjunto* definível de A^n, adotado por [Hodges].)

Lembramos que o fato de θ ser uma fórmula de equivalência pode ser escrito como uma sentença de L, de modo que θ será fórmula de equivalência também em toda estrutura elementarmente equivalente a $\mathfrak{A}$.

Defina A^{eq} como a união (disjunta) dos conjuntos I_θ formados por fórmulas de equivalência θ. (Por união disjunta, entendemos que os conjuntos I_θ são dois a dois disjuntos por imposição, por exemplo tomando $A^{\mathrm{eq}} = \bigcup_\theta I_\theta \times \{\theta\}$.) Podemos entender que $A^n \subseteq A^{\mathrm{eq}}$ identificando $a \in A^n$ com sua classe unitária $a/(x = y)$ e A^n com $I_{(x=y)}$.

Exemplo 4.3.1. Este é o Exemplo 4 da Seção 4.3 de [Hodges]. Suponha que V é um espaço vetorial de dimensão 3 sobre um corpo finito. Podemos escrever uma fórmula $\theta(x, y)$ que afirme que x e y são vetores não-nulos linearmente dependentes (ou paralelos); a fórmula θ é de equivalência e I_θ corresponde ao conjunto de pontos da geometria projetiva de V no Exemplo 3.3.5. Também podemos escrever uma fórmula $\eta(x_1, x_2, y_1, y_2)$ que afirme que $\{x_1, x_2\}$ e $\{y_1, y_2\}$ são bases do mesmo subespaço; também η é de equivalência e I_η corresponde ao conjunto de retas da geometria projetiva. Os predicados Q_θ e Q_η permitem definir a relação de incidência dessa geometria, de modo que afirmações sobre a geometria podem ser traduzidas como afirmações sobre V^{eq}.

Para cada fórmula de equivalência θ, sendo n qualquer, adicione a L um predicado unário P_θ e um binário Q_θ, obtendo a linguagem L^{eq}. Note que $|\mathrm{L}^{\mathrm{eq}}| = |\mathrm{L}|$. Interprete P_θ como I_θ e Q_θ como o gráfico de f_θ, isto é, $f_\theta \subseteq I_{(x=y)} \times I_\theta$. Interprete os predicados n-ários de L nas classes de $I_{(x=y)}$ via identificação (para cada n). Obtemos assim a L^{eq}-estrutura $\mathfrak{A}^{\mathrm{eq}}$.

(Como $I_{(x=y)}$ não é todo o conjunto A^{eq}, surge aqui a necessidade de L não ter operadores.)

Note que os conjuntos I_θ são *tipos* de $\mathfrak{A}^{\mathrm{eq}}$, embora aqui não façamos uso de linguagens de múltiplos tipos (Em inglês, *sorts* e *many-sorted logics* respectivamente.). A linguagem torna-se imperativamente de múltiplos tipos se desejarmos usar diretamente os operadores f_θ em vez dos predicados Q_θ; como a distinção é sutil, porém, podemos permanecer com L^{eq} de primeira ordem e ainda escrever f_θ para abreviar fórmulas com Q_θ. Porém, cada variável de uma fórmula só poderá ser interpretada por elementos de um I_θ: ou redefine-se a construção das fórmulas introduzindo sempre a verificação $P_\theta(v)$ ou assume-se que as fórmulas com que se trabalha estão adequadas a essa exigência. É esta nossa postura.

Como observamos, se $\mathfrak{A} \equiv \mathfrak{B}$ então as fórmulas de equivalência são as mesmas para ambas as estruturas, e L^{eq} é a mesma. Vemos que $\mathfrak{A} \equiv \mathfrak{B} \Leftrightarrow \mathfrak{A}^{\mathrm{eq}} \equiv$

$\mathfrak{B}^{eq}$ e, se $\mathfrak{A} \prec \mathfrak{B}$, então $\mathfrak{A}^{eq} \prec \mathfrak{B}^{eq}$. Portanto, se T é uma teoria completa de L com modelo $\mathfrak{A}$, consideramos $T^{eq} = Th(\mathfrak{A}^{eq})$. Também se definem $\mathrm{dcl}^{eq}(X)$ e $\mathrm{acl}^{eq}(X)$ os fechos correspondentes de $X \subseteq A^{eq}$.

A teoria T^{eq} equivale a T com as sentenças que afirmam que, para cada fórmula de equivalência θ, f_θ é sobrejetora sobre I_θ e $f_\theta(x) = f_\theta(y) \leftrightarrow \theta(x,y)$.

Note que todo automorfismo de $\mathfrak{A}$ estende-se, de maneira natural e única, a um automorfismo de $\mathfrak{A}^{eq}$; por outro lado, todo automorfismo de $\mathfrak{A}^{eq}$ restringe-se a um automorfismo de $\mathfrak{A}$. Escrevem-se, portanto, DCL^{eq} e ACL^{eq} quando se considera toda $\mathfrak{A}^{eq}$.

Finalmente, todo subconjunto de A^m definível em $\mathfrak{A}^{eq}$ é definível em $\mathfrak{A}$ e, reciprocamente,

Proposição 4.3.2. Uma estrutura interpretável em $\mathfrak{A}$ é definível em $\mathfrak{A}^{eq}$.

Demonstração: Suponha U e $\sim$ como na definição. Suponha que U e $\sim$ são definidos por fórmulas $\phi(x)$ e $\psi(x,y)$ respectivamente, sem parâmetros. Então

$$\theta(x,y) : (\phi(x) \wedge \phi(y) \wedge \psi(x,y)) \vee (x = y)$$

é uma fórmula de equivalência, com as classes de $\sim$ e mais uma para cada elemento do complemento de U.

Suponha que $\chi(u_1, \ldots, u_k)$ define, também sem parâmetros, uma relação em U que independe dos representantes de $\sim$, sendo $u_1, \ldots, u_k$ seqüências de n variáveis. Defina, com variáveis $v_1, \ldots, v_k$, a fórmula de L^{eq}

$$\pi(v_1, \ldots, v_k) : \exists u_1 \ldots \exists u_k \, (Q_\theta(u_1, v_1) \wedge \ldots \wedge Q_\theta(u_k, v_k) \wedge \chi(u_1, \ldots, u_k)) \,.$$

Dadas $a_1, \ldots, a_k \in A^n$, se $\mathfrak{A} \models \chi(a_1, \ldots, a_k)$ então $\mathfrak{A}^{eq} \models \pi(a_1/\theta, \ldots, a_k/\theta)$, tomando $a_i/(x = y)$ para interpretar u_i. Reciprocamente, se $\mathfrak{A}^{eq} \models \pi(a_1/\theta, \ldots, a_k/\theta)$, então existem $b_1, \ldots, b_k \in A^n$ tais que $b_i \sim_\theta a_i$ e $\mathfrak{A} \models \chi(b_1, \ldots, b_k)$. Vem $(b_1, \ldots, b_k) \in U^k$ e cada $b_i \sim a_i$, de modo que $(a_1, \ldots, a_k) \in U^k$ e $\mathfrak{A} \models \chi(a_1, \ldots, a_k)$. QED

Mencionamos apenas, como observado pela Seção 16.4 de [Poizat 1], que a correspondência $(\cdot)^{eq}$ é uma bijeção entre modelos de uma teoria completa T e modelos de T^{eq} que omitem o tipo p_∞ que contém as fórmulas $\neg P_\theta$; se $\mathfrak{A}$ é κ-saturada então $\mathfrak{A}^{eq}$ o é para tipos que não contenham p_∞; se T é κ-estável então T^{eq} também o é; segundo [Pillay], se $\mathfrak{A}$ é κ-grande, com κ cardinal infinito, também $\mathfrak{A}^{eq}$ é κ-grande.

Sabemos que, se ψ é uma fórmula de L com m variáveis livres e $a \in A^m$, então $\mathfrak{A} \models \psi(a) \Leftrightarrow \mathfrak{A}^{eq} \models \psi(a)$. Explorar situações análogas nos impele a adaptar o Teorema 4.3.3 de [Hodges]:

Teorema 4.3.3. (i) Cada A^n e as relações, operadores e constantes de $\mathfrak{A}$ são $\emptyset$-definíveis em $\mathfrak{A}^{\mathrm{eq}}$.

(ii) Se $\mathfrak{B} \prec \mathfrak{A}$, então $B^{\mathrm{eq}} = \mathrm{dcl}^{\mathrm{eq}}(B) = \mathrm{acl}^{\mathrm{eq}}(B)$.

(iii) Para toda fórmula $\phi(x_1, \ldots, x_n)$ de L^{eq}, com x_i variável de tipo I_{θ_i}, existe $\psi(y_1, \ldots, y_n)$ fórmula de L que equivale a $\phi(\pi_{\theta_1}(y_1), \ldots, \pi_{\theta_n}(y_n))$ em T^{eq}. A fórmula ψ independe da particular L-estrutura $\mathfrak{A}$. Em particular, se ϕ tem uma única variável livre e de tipo $I_{(x=y)}$, para cada $a \in A^n$ vale $\mathfrak{A}^{\mathrm{eq}} \models \phi(a/(x = y)) \Leftrightarrow \mathfrak{A} \models \psi(a)$.

(iv) Uma imersão elementar $h : \mathfrak{A} \to \mathfrak{B}$ estende-se naturalmente a uma imersão elementar $h^{\mathrm{eq}} : \mathfrak{A}^{\mathrm{eq}} \to \mathfrak{B}^{\mathrm{eq}}$, sendo o mesmo verdade para subestruturas por simetria. Em particular, se h é a identidade, também h^{eq} é a identidade.

(v) Se $X \subseteq A$, então qualquer dos operadores dcl, acl, DCL, ACL satisfaz $\mathrm{cl}(X) = \mathrm{cl}^{\mathrm{eq}}(X) \cap A$.

Demonstração: É preciso ter em mente a identificação $a : a/(x = y)$.

(i) A fórmula atômica $P_{(x=y)}$ define A^n. Se P é um predicado n-ário de L, então $P_{P(x) \wedge P(y)}$ define $R^{\mathfrak{A}}$. Se f é um operador n-ário de L, então $Q_{(f(x)=f(y))}$ define o gráfico de $f^{\mathfrak{A}}$. Se c é uma constante de L, então $P_{(x=c)\wedge(y=c)}$ define $c^{\mathfrak{A}}$.

(ii) Dado a/θ para $a \in A^n$, a fórmula $Q_\theta(a/(x = y), v)$ define a/θ.

(iii) No caso particular, para cada fórmula de equivalência θ, devemos expandir P_θ, Q_θ assim: substitua $P_\theta(v)$ por $\theta(v_1, \ldots, v_n, v_1, \ldots, v_n)$ e $Q_\theta(u, v)$ por $\theta(u_1, \ldots, u_n, v_1, \ldots, v_n)$.

Em geral, note que $\phi(\pi_{E_1}(y_1), \ldots, \pi_{E_n}(y_n))$ abrevia a fórmula de L^{eq}

$$\forall z_1 \ldots \forall z_n \left(\phi(z_1, \ldots, z_n) \leftrightarrow \left(Q_{\theta_1}(y_1, z_1) \wedge \ldots \wedge Q_{\theta_n}(y_n, z_n)\right)\right).$$

(iv) A função $h^{\mathrm{eq}} : A^{\mathrm{eq}} \to B^{\mathrm{eq}}$, $h^{\mathrm{eq}}(a/\theta) = h(a)/\theta$, está bem-definida.

(v) Como L^{eq} expande L, temos $\mathrm{acl}(X) \subseteq \mathrm{acl}^{\mathrm{eq}}(X), A$. Suponha $x \in \mathrm{acl}^{\mathrm{eq}}(X) \cap A$: então $x \in \phi(\mathfrak{A}^{\mathrm{eq}}, a)$ finito com a seqüência de parâmetros em X e ϕ fórmula de L^{eq}. Por (iii), existe ψ de L tal que, para todo $\alpha \in A$, $\mathfrak{A}^{\mathrm{eq}} \models \phi[\alpha, a] \Leftrightarrow \mathfrak{A} \models \psi(\alpha, a)$. Então $\psi(\mathfrak{A}, a)$ é finito e contém x, donde $x \in \mathrm{acl}(X)$. O mesmo raciocínio val no caso do fecho definível. Obtém-se o resultado para $\mathrm{DCL}^{\mathrm{eq}}$ e $\mathrm{ACL}^{\mathrm{eq}}$ por suas definições. QED

Repetir a construção "eq" apenas considera fórmulas de equivalência sobre classes de equivalência e é, portanto, redundante (Exercício 4.3.5 de [Hodges] ou Lema 16.13 de [Poizat 1]).

4.4. Bases canônicas

Para relacionar a propriedade de modularidade local (baseada em pré-geometrias) e a geometria de curvas, faremos uso de conceitos e resultados que exporemos nesta seção. Adaptamos a Seção 8.2 de [Marker].

Fixada a L-estrutura $\mathfrak{A}$, consideraremos também $\mathfrak{A}^{\mathrm{eq}}$. Sabemos que os automorfismos de $\mathfrak{A}$ e $\mathfrak{A}^{\mathrm{eq}}$ são essencialmente os mesmos, identificados simplesmente como "automorfismos".

Para relacionar automorfismos e definíveis no Lema 4.4.3, assumiremos que $\mathfrak{A}^{\mathrm{eq}}$ é um modelo monstro em que $\mathrm{dcl}^{\mathrm{eq}}$ e $\mathrm{DCL}^{\mathrm{eq}}$ coincidem para qualquer $X \subseteq A^{\mathrm{eq}}$, estrutura que pode não existir. No Teorema 4.4.5, obteremos implicitamente uma limitação da cardinalidade dos conjuntos, a qual podemos aplicar a Proposição 3.1.9 e considerar um modelo monstro de grandeza especificada.

No Exemplo 1.3.15, vimos que se $p \in S_m^{\mathfrak{A}}(A)$ e σ é automorfismo de $\mathfrak{A}$, então $\sigma \cdot p = \{\sigma[D] \subseteq A^m \mid D \in p\}$ também é um tipo sobre A, de modo que se definiu uma ação do grupo dos automorfismos sobre o espaço $S_m^{\mathfrak{A}}(A)$.

Definição 4.4.1. (i) Suponha $D \in \mathrm{Def}^m_{\mathfrak{A},A}$ e $P \subseteq A^{\mathrm{eq}}$. Diz-se que P é um *parâmetro (ou base) canônico*de D se os automorfismos que fixam D são precisamente os que fixam os elementos de P.

(ii) Suponha $p \in S_m^{\mathfrak{A}}(A)$ e $P \subseteq A^{\mathrm{eq}}$. Diz-se que P é um *parâmetro (ou base) canônico* de p se os automorfismos que fixam p são precisamente os que fixam os elementos de P.

Lema 4.4.2. Dados $X \subseteq A$ e $D \in \mathrm{Def}^m_{\mathfrak{A},X}$, existe $\alpha \in \mathrm{dcl}^{\mathrm{eq}}(X)$ tal que $\{\alpha\}$ é um parâmetro canônico de D.

Demonstração: Seja $\phi(v,w)$ fórmula de L e $a \in X^n$ tais que $D = \phi(\mathfrak{A}, a)$. Considere a relação binária definida em A^n por $\theta(x,y) : \forall v\,(\phi(v,x) \leftrightarrow \phi(v,y))$. Tome $\alpha = (a/\theta) \in \mathrm{dcl}^{\mathrm{eq}}(X)$, identificando-se (a/θ) e $a \in X^n$.

Mostremos que $\{\alpha\}$ é um parâmetro canônico de D. Seja σ um automorfismo. Se σ fixa α e $\mathfrak{A}^{\mathrm{eq}} \models \phi(x,\alpha)$, então $\mathfrak{A}^{\mathrm{eq}} \models \phi(\sigma(x),\alpha)$, de modo que σ fixa D. Suponha então que σ fixa D. Para todo x adequado, portanto, $\mathfrak{A}^{\mathrm{eq}} \models \phi(x,\alpha) \Rightarrow \mathfrak{A}^{\mathrm{eq}} \models \phi(\sigma(x),\alpha)$, donde $\mathfrak{A}^{\mathrm{eq}} \models \phi(x,\alpha) \Rightarrow \mathfrak{A}^{\mathrm{eq}} \models \phi(\sigma^{-1}(x),\alpha)$ e $\mathfrak{A} \models \forall u\,(\psi(u,a) \rightarrow \psi(u,\sigma^{-1}(a)))$. Assim, $\mathfrak{A} \models \forall u\,(\psi(u,\sigma(a)) \rightarrow \psi(u,a))$. Como $\sigma[D] = D$, vem $\mathfrak{A} \models \theta(\sigma(a),a)$ e σ fixa α. QED

Lema 4.4.3. Suponha que $P \subseteq A^{\mathrm{eq}}$ é um parâmetro canônico de $p \in S_m^{\mathfrak{A}}(A)$. Então $Q \subseteq A^{\mathrm{eq}}$ é parâmetro canônico de p se e somente se $\mathrm{dcl}^{\mathrm{eq}}(Q) = \mathrm{dcl}^{\mathrm{eq}}(P)$. Em particular, $\mathrm{dcl}^{\mathrm{eq}}(P)$ é o maior parâmetro canônico de p.

Demonstração: Não afirmamos, ainda, que P existe. Assumiremos que, para qualquer $Q \subseteq A^{\mathrm{eq}}$, $\mathrm{dcl}^{\mathrm{eq}}(Q) = \mathrm{DCL}^{\mathrm{eq}}(Q)$ é o conjunto dos elementos de A^{eq} fixados pelos automorfismos que fixam os elementos de Q.

Se Q é um parâmetro canônico e σ é um automorfismo fixando seus elementos, então $\sigma p = p$ e σ fixa os elementos de P, de modo que $P \subseteq \mathrm{dcl}^{\mathrm{eq}}(Q)$.

Analogamente, $Q \subseteq \mathrm{dcl}^{\mathrm{eq}}(P)$ e obtemos $\mathrm{dcl}^{\mathrm{eq}}(P) = \mathrm{dcl}^{\mathrm{eq}}(Q)$.

Reciprocamente, suponha $\mathrm{dcl}^{\mathrm{eq}}(P) = \mathrm{dcl}^{\mathrm{eq}}(Q)$. Os automorfismos que fixam os elementos de P são precisamente aqueles que fixam os elementos de Q. Já que P é um parâmetro canônico de p, também Q o é. QED

Para $p \in S_m^{\mathfrak{A}}(A)$ e $P \subseteq A^{\mathrm{eq}}$, esse lema permite-nos enunciar a

Definição 4.4.4. Se P é um parâmetro canônico de p, definimos a *base canônica* de p como $\mathrm{cb}(p) = \mathrm{dcl}^{\mathrm{eq}}(P)$. (Em inglês, cb abrevia *canonical base.*) Lembre que se trata do maior parâmetro canônico de p.

Teorema 4.4.5. Suponha que p é definível. Então p tem um parâmetro canônico. Se p não se desvia sobre $X \subseteq A$, então existe $\alpha \in \mathrm{acl}^{\mathrm{eq}}(X)$ tal que $\{\alpha\}$ é um parâmetro canônico de p; caso $p|_X$ seja estacionário, podemos tomar $\alpha \in \mathrm{dcl}^{\mathrm{eq}}(X)$. Em cada dessas condições, portanto, existe $\mathrm{cb}(p)$.

Referência: O Teorema 8.2.7 de [Marker].

Introduziremos agora a geometria de curvas que relacionaremos à propriedade de modularidade local.

Definição 4.4.6. Suponha $D \in \mathrm{Def}^1_{\mathfrak{A},A}$ fortemente minimal, $E \in \mathrm{Def}^1_{\mathfrak{A},A}$ e $C \subseteq D^2 \times E$ definível. Diz-se que C é uma *família de curvas planas* se, para todo $e \in E$, a *curva* $C_e = \{d \in D^2 \mid (d, e) \in C\}$ é um subconjunto fortemente minimal de D^2.

Definição 4.4.7. Suponha $D \in \mathrm{Def}^1_{\mathfrak{A},A}$ fortemente minimal definido por uma fórmula parametrizada $\psi(v)$. Diz-se que D é *linear* se, para todo $p \in S_2(D)$, se $\psi(v_1) \wedge \psi(v_2) \in p(v_1, v_2)$ e $\mathrm{RM}(p) = 1$, a base canônica de p tem posto no máximo 1. (O *posto* de uma base canônica é o menor ξ tal que existe parâmetro canônico $b \in A^{\mathrm{eq}}$ tal que $\mathrm{RM}(b) = \xi$.)

Suponha que $D = \phi(\mathfrak{A}, a)$, em que a é uma seqüência de parâmetros, é fortemente minimal. Considere a família $\mathscr{C}$ dos conjuntos $C_b = \{(x, y) \in D^2 \mid \mathfrak{A} \models \phi(x, y, b)\}$, em que a e b têm o mesmo tipo sobre D. Então a relação de equivalência $C_b =_1 C_c$ em $\mathscr{C}$ é definível — lembre que $E =_1 F \Leftrightarrow \mathrm{RM}(E \triangle F) < 1 \Leftrightarrow E \triangle F$ é finito. Seja p o tipo determinado por D: então o posto da base canônica de p corresponde intuitivamente à dimensão de $\mathscr{C}$ quocientada pela equivalência $=_1$. Assim, D é linear se e somente se não existe uma família de curvas planas de dimensão maior que 1. Corpos algebricamente fechados não são lineares, porque existe a família de curvas $C_{ab} = \{(x, y) \mid y = ax + b\}$. Espaços vetorias são lineares.

Teorema 4.4.8. Suponha $D \in \mathrm{Def}^1_{\mathfrak{A},A}$ fortemente minimal. Equivalem:

(i) Para algum $B \subseteq D$, a pré-geometria D/B é modular.

(ii) D é linear.

(iii) Para todo $b \in \mathrm{acl}(\emptyset)$, $D/\{b\}$ é modular.

(iv) D é localmente modular.

Referência: O Teorema 8.2.11 de [Marker].

Agora enunciamos uma definição melhor justificada pelo lema que a segue:

Definição 4.4.9. Dizemos que $\mathfrak{A}$ é *um-baseada* se, para cada $X, Y \subseteq A^{\mathrm{eq}}$ com $X = \mathrm{acl}^{\mathrm{eq}}(X)$ e $Y = \mathrm{acl}^{\mathrm{eq}}(Y)$, vale $X \mathop{\perp\!\!\!\perp}_{X \cap Y} Y$.

Lema 4.4.10. $\mathfrak{A}$ é um-baseada se e somente se, para cada $a \in (A^{\mathrm{eq}})^m$ e $Y \subseteq A^{\mathrm{eq}}$ tais que $t(a/Y)$ é estacionário, $\mathrm{cb}(t(a/Y)) \subseteq \mathrm{acl}^{\mathrm{eq}}(a)$.

Referência: O Lema 8.2.13 de [Marker].

Teorema 4.4.11. Suponha que A é fortemente minimal. Então $\mathfrak{A}$ é um-baseada se e somente se A é localmente modular.

Referência: O Teorema 8.2.14 de [Marker].

4.5. Eliminação de imaginários

Definição 4.5.1. Uma teoria tem *eliminação de imaginários* se, em qualquer modelo seu, todo definível tem um parâmetro canônico.

Como a construção "eq" não precisa ser repetida, por não acrescentar novas informações, obtemos a

Proposição 4.5.2. T^{eq} tem eliminação de imaginários.

Demonstração: Suponha $D_{\mathrm{eq}} = \phi(\mathfrak{A}^{\mathrm{eq}}, a_1/\theta_1, \ldots, a_n/\theta_n)$, em que ϕ é uma linguagem de L^{eq}. Podemos transformar ϕ em uma fórmula ψ de L e trabalhar com $D = \psi(\mathfrak{A}, a_1, \ldots, a_n)$ no Lema 4.4.2 QED

A teoria *ACF* tem eliminação de imaginários, como mostram as p. 63–64 de [Pillay A] e o Exercício 3.4.19 e as p. 91–93 de [Marker].

5
Grupos totalmente transcendentais

Trabalharemos com uma linguagem fixada L que expanda a dos grupos. Suporemos que G é um grupo com estrutura adicional $(G, \ldots)$ apropriada para L e que essa estrutura, ou a teoria $Th(G, \ldots)$, é totalmente transcendental, dizendo-se simplesmente que G é *totalmente transcendental*. De fato, a letra G refere-se ao grupo G e também a toda a estrutura $(G, \ldots)$. Estudaremos os grupos definíveis em uma seção específica, com hipóteses próprias.

O produto por um elemento é uma bijeção definível, de modo que classes laterais e outros produtos de conjuntos têm presença constante. Portanto, alertamos que, neste capítulo, justaposições como Ha ou B_1B_2 têm seu significado usual de produtos $Ha = \{ha \mid h \in H\}$ (classe lateral, conhecida em inglês como *coset*) e $B_1B_2 = \{b_1b_2 | b_i \in B_i\}$ e ***não*** devem ser confundidas com a justaposição $XYa = X \cup Y \cup \{a\}$, que não adotaremos aqui.

Ao considerar subgrupos e quocientes de G como L-estruturas, nossas afirmações têm implícitas as respectivas hipóteses de que o subgrupo considerado seja subestrutura de G por toda L e que as relações, operadores e constantes de G independam dos elementos equivalentes pelo subgrupo normal.

Com algumas adaptações, este capítulo segue aproximadamente [Lascar]. A teoria básica de grupos com que lidaremos é a usual dos cursos introdutórios de Álgebra, com tópicos como subgrupos (normais) e ações, e está contida no primeiro capítulo de [Lang] e [Jacobson I].

O leitor encontrará, em boa parte da literatura, o estudo de grupos *estáveis* ou *ω-estáveis* e títulos correspondentes. Concordamos com [Hodges] e optamos por destacar a propriedade que realmente usaremos, embora muitas propriedades admitam demonstrações mais complexas para o caso estável. Referências abrangentes são [Poizat 2] e F. O. Wagner, *Stable Groups*, Cambridge University Press, 1997.

5.1. Subgrupos definíveis

Tradicionalmente, esta seção teria o título "Condição de cadeia descendente", mas tal condição será apenas usada para demonstrar que a intersecção de subgrupos definíveis de G é a intersecção de um número finito deles, propriedade da qual faremos maior uso.

Como G é totalmente transcendental, existem o posto e o grau de Morley de qualquer subconjunto definível não-vazio de G — caso dos subgrupos definíveis. Esse fato é importante em algumas das próximas demonstrações.

Esta primeira observação é simples e crucial.

Lema 5.1.1. Suponha que H é um subgrupo definível de G e $a \in G$ é qualquer. Então $\mathrm{RM}(Ha) = \mathrm{RM}(aH) = \mathrm{RM}(H)$ e $\mathrm{dM}(Ha) = \mathrm{dM}(aH) = \mathrm{dM}(H)$.

Demonstração: Basta notar que Ha e aH também são definíveis e que multiplicação por a, a qualquer lado, é uma bijeção definível. QED

Corolário 5.1.2. Suponha H, K subgrupos definíveis de G com $H \subseteq K$. Se $[K:H]$ é infinito, então $\mathrm{RM}(K) > \mathrm{RM}(H)$; se $[K:H]$ é finito, então $\mathrm{RM}(K) = \mathrm{RM}(H)$ e $\mathrm{dM}(K) = [K:H]\,\mathrm{dM}(H)$.

Demonstração: No primeiro caso, há infinitas classes laterais de H contidas em K, definíveis duas a duas disjuntas, todas com mesmo posto. Trabalhando em uma extensão ω-saturada de G, usamos a definição de posto interno para obter a desigualdade.

No caso finito, temos uma partição $K = Ha_1 \cup \ldots \cup Ha_n$, em que $a_1 = 1$ e todas as classes têm mesmo posto e grau. Assim, $\mathrm{dM}(K) = \sum_{i=1}^{n} \mathrm{dM}(Ha_i) = n\,\mathrm{dM}(H)$, mas $n = [K:H]$. QED

Corolário 5.1.3. Se $(H_n)_{n\in\mathbb{N}}$ é uma cadeia decrescente de subgrupos definíveis de G, então existe $n_0 \in \mathbb{N}$ tal que $H_n = H_{n_0}$ para todo $n \geqslant n_0$.

Demonstração: Como para tipos, tome n_0 tal que H_{n_0} tenha posto mínimo pela boa ordem dos ordinais e grau mínimo pela boa ordem dos naturais dentre os que têm posto mínimo. O corolário anterior impede que haja outro subgrupo na cadeia propriamente contido em H_{n_0}. QED

Eis a "propriedade de intersecção":

Proposição 5.1.4. A intersecção de qualquer família não-vazia de subgrupos definíveis de G é igual à intersecção de uma subfamília finita, de modo que é definível.

Demonstração: Suponha que $\mathscr{F}$ seja uma família infinita de subgrupos definíveis cuja intersecção não coincide com a de qualquer subfamília finita. Definamos indutivamente uma cadeia de elementos de $\mathscr{F}$, assim: tome $H_0 \in \mathscr{F}$ qualquer; definidos $H_0, \ldots, H_n \in \mathscr{F}$, por hipótese $H_0 \cap \ldots \cap H_n \neq \bigcap \mathscr{F}$, existindo $H_{n+1} \in \mathscr{F}$ com $H_0 \cap \ldots \cap H_n \neq H_0 \cap \ldots \cap H_n \cap H_{n+1}$. Obtemos uma cadeia $(\bigcap_{i \leqslant n} H_i)_{n\in\mathbb{N}}$ de subgrupos definíveis de G, decrescente que não estaciona, contradição. QED

Desse modo, *qualquer* cadeia decrescente de subgrupos definíveis de G estaciona em "comprimento" *finito*.

Exemplo 5.1.5. Se A é qualquer subconjunto de G, define-se seu centralizador $Z(A) = \{g \in G \mid ga = ag$ para todo $a \in A\} = \bigcap_{a \in A} Z(a)$, em que $Z(a) = \{g \in G \mid ga = ag\}$. Mas cada $Z(a)$ é $\{a\}$-definível, de modo que $Z(A)$ é o centralizador de um subconjunto finito de A e é definível.

Agora, suponha $\phi(u), \psi(v, u)$ fórmulas de L(G) tais que, se $g \in G$ satisfaz ϕ, então $\psi(G, g)$ é um subgrupo de G. Então $\forall u\, (\phi(u) \to \psi(v, u))$ define a intersecção de todos esses subgrupos, que também é definida por uma conjunção finita $\psi(v, g_1) \wedge \ldots \wedge \psi(v, g_n)$. Ambas as fórmulas definem a mesma intersecção em qualquer extensão elementar de G, porque equivalem em G.

Por exemplo, seja A um subconjunto de G definido pela fórmula $\alpha(u)$, ou seja, $A = \alpha(G)$. Então $Z(A)$ é definido por $\forall u\, (\alpha(u) \to (vu = uv))$, que define em qualquer extensão elementar G_1 de G o centralizador de $\alpha(G_1)$. Vimos no exemplo anterior que existem $a_1, \ldots, a_n \in A$ tais que $Z(A)$ é definido por $\bigwedge_{i=1}^{n}(a_i v = v a_i)$, de modo que essas duas fórmulas equivalem em G, e então em qualquer extensão (ou restrição contendo os parâmetros adequados) elementar de G. Assim, o centralizador do conjunto definido por α é o mesmo de $\{a_1, \ldots, a_n\}$.

Definição 5.1.6. Um subgrupo definível de G é *conexo* se não contém subgrupo definível próprio de índice finito.

Se G é conexo e N é um subgrupo normal, então G/N é conexo.

Lema 5.1.7. G tem um menor subgrupo definível de índice finito, portanto conexo, indicado G^0 e chamado *componente conexa* de G. (Veja comentário na pág. 153.) Note que $\mathrm{RM}(G^0) = \mathrm{RM}(G)$.

Demonstração: A intersecção de todos os subgrupos definíveis de índice finito de G é igual à intersecção G^0 de um número finito deles. Mas então G^0 é um subgrupo definível de índice finito. QED

Na próxima seção, calcularemos $\mathrm{dM}(G^0) = 1$ e $\mathrm{dM}(G) = [G : G^0]$.

Corolário 5.1.8. G^0 é um subgrupo normal de G.

Demonstração: Para qualquer $g \in G$, gG^0g^{-1} é um subgrupo definível com índice $[G : G^0]$, donde $G^0 = gG^0g^{-1}$. QED

Explicitemos um lema técnico:

Lema 5.1.9. Sejam u uma única variável e v uma seqüência arbitrária (finita). Para quaisquer $\theta(u, v)$ fórmula de L e $n \in \mathbb{N}^*$, existe uma fórmula $\theta'(v)$

de L expressando que $\theta(G)(v)$ é um subgrupo de índice n de G quando v é interpretada.

Demonstração: De fato, θ' é a conjunção de

$$\forall u_1 \forall u_2 \, (\theta(u_1, v) \wedge \theta(u_2, v) \rightarrow \theta(u_1 u_2, v) \wedge \theta(u_1^{-1}, v)) \wedge \theta(1, v) \ ,$$

que expressa "$\theta(G)(v)$ é um subgrupo de G", e

$$\exists a_1 \ldots \exists a_n \, (\bigwedge_{i \neq j} \neg\theta(a_i a_j^{-1}, v) \wedge \forall w \bigvee_{i=1}^{n} \theta(w a_i^{-1}, v)) \ ,$$

que expressa que esse subgrupo tem n classes laterais. QED

Proposição 5.1.10. A componente conexa G^0 é $\emptyset$-definível e a fórmula sem parâmetros ϕ^0 que define G^0 em G satisfaz, para $G_1 \equiv G$, $(G_1)^0 = \phi^0(G_1)$.

Demonstração: Sejam $\phi(u, v)$ uma fórmula de L e a uma seqüência de elementos de G de modo que $G^0 = \phi(G, a)$. Seja $k = [G : G^0]$.

Pelo lema, existe uma fórmula $\psi(v)$ de L tal que $G \models \psi(b)$ se e somente se $\phi(G, b)$ é um subgrupo de G de índice k. Assim, $G \models \psi(a)$ e $G \models \psi(b) \Leftrightarrow \phi(G, b) = G^0$, de modo que $\phi^0(u) : \exists v \, (\psi(v) \wedge \phi(u, v))$ define G^0.

Note ainda que, por $\phi^0(G)$ ser conexo, G satisfaz, para cada $\xi(u, v)$ fórmula de L e $n > k$, a sentença (fornecida pelo lema) que expressa

$$\neg \exists v \, (\xi(u, v) \wedge \phi^0(u)) \text{ "define um subgrupo de índice } n\text{"}.$$

($\xi \wedge \phi^0$ definiria qualquer subconjunto definível de G^0 com parâmetros v.)

G_1 satisfaz essas sentenças e também a que expressa "$\phi^0(u)$ define um subgrupo de índice k". Assim, ϕ^0 define a componente conexa de G_1. QED

Corolário 5.1.11. Se G é conexo, então qualquer grupo elementarmente equivalente a G é conexo.

Basta observar que $G = G^0 \Leftrightarrow G \models \forall u \, \phi^0(u)$.

5.2. O espaço dos 1-tipos globais

Recorde que, para os tipos de $S_1(G)$, as hipóteses (das seções) dos Teoremas 2.4.4 e 2.6.8 são verificadas: cada tipo é definível, tem grau 1 e uma única extensão direta, que é seu único herdeiro e com o mesmo esquema de definição.

Introduziremos uma ação de G no espaço $S_1(G)$, mas faremos uso apenas de fatos básicos a respeito de ações: o estabilizador *Stab*(p) é indicado G_p na Seção I.5 de [Lang], em que é chamado *grupo de isotropia*; Stab p na Seção 1.12 de [Jacobson I]; Fix(p) em [Poizat 2], que o chama *fixer* em inglês.

Primeiramente observe que, se u, v são variáveis, $g \in G$ e $\phi(u)$ é uma fórmula de $L(G)$, então a fórmula obtida substituindo-se u pelo termo gv é também uma fórmula de $L(G)$, que escrevemos $\phi(gv)$.

Seja $D = \phi(G) = \{x \in G \mid G \models \phi(x)\}$. O conjunto definido por $\phi(gv)$ é $\phi(g(G)) = \{x \in G \mid G \models \phi(gx)\} = \{x \in G \mid gx \in D\} = g^{-1}D$. Temos $\mathrm{RM}(g^{-1}D) = \mathrm{RM}(D)$ pela invariância por bijeção definível, valendo também a igualdade análoga para grau, caso exista ($D \neq \emptyset$).

Suponha agora $p \in S_1(G)$ e defina $g \cdot p = \{\phi \mid \phi(gv) \in p(v)\}$. Notamos que $g \cdot p = \{\psi(g^{-1}v) \mid \psi \in p\}$, porque p é fechado sob equivalência, ou seja, $(g \cdot p)(v) = p(g^{-1}v)$. Este modo de escrever $g \cdot p$ será muito útil para alguns cálculos. Por exemplo, suponha que um elemento a de uma extensão elementar de G satisfaça p: então ga satisfaz $g \cdot p$.

Em termos de definíveis, obtemos $g \cdot p = \{D \mid g^{-1}D \in p\} = \{gE \mid E \in p\}$.

Desse modo, $g \cdot p \in S_1(G)$, porque g também é um parâmetro de G e satisfazem-se as propriedades de fechamento sob intersecção e continência e de complementação. Temos ainda $\mathrm{RM}(g \cdot p) = \mathrm{RM}(p)$ e $\mathrm{dM}(g \cdot p) = \mathrm{dM}(p) = 1$.

O que definimos é uma ação de G em $S_1(G)$. Temos diretamente $1 \cdot p = p$ e, com cuidado, calculamos $g \cdot (h \cdot p) = g \cdot \{\phi(h^{-1}w) \mid \phi \in p\} = \{\phi(h^{-1}(g^{-1}v)) \mid \phi \in p\} = \{\phi((gh)^{-1}v) \mid \phi \in p\} = (gh) \cdot p$.

Como em toda ação, somos levados a considerar o estabilizador $Stab(p) = \{g \in G \mid g \cdot p = p\}$.

Proposição 5.2.1. *$Stab(p)$ é um subgrupo definível de G. Se $G \prec G_1$ e p_1 é o herdeiro de p sobre G_1, então $Stab(p_1)$ é definido em G_1 pela fórmula que define $Stab(p)$ em G.*

Demonstração: Suponha que $\phi(v)$ seja uma fórmula de $L(G)$ cujo definível determine p. Afirmamos que $g \in Stab(p) \Leftrightarrow \phi(g^{-1}v) \in p$. Sendo a implicação direta imediata, lembre-se que, se $\phi(g^{-1}v) \in p$, temos $\phi(v) \in g \cdot p$. Mas $g \cdot p$ e p têm mesmos posto e grau, ou seja, $\phi(G)$ determina também $g \cdot p$.

Contudo, escrevendo $\theta(v, u) : \phi(u^{-1}v)$, temos $\phi(g^{-1}v) \in p \Leftrightarrow G \models d_p\theta(g)$, de modo que $d_p\theta$ define $Stab(p)$.

Com respeito a G_1, o Teorema 2.6.8 mostra que p_1 é determinado por $\phi(G_1)$. Assim, novamente $Stab(p_1) = \{g_1 \in G_1 \mid \phi(g_1^{-1}v) \in p_1\}$ e $\phi(g_1^{-1}v) \in p_1 \Leftrightarrow G_1 \models d_p\theta(g_1)$. QED

Proposição 5.2.2. *Sempre $Stab(p) \subseteq G^0$.*

Demonstração: Suponha $g \in Stab(p)$ e seja a uma realização de p em uma extensão elementar G_1 de G. Seja ϕ^0 a fórmula que define G^0. Então existem $c_1, \ldots, c_k \in G$, sendo $k = [G : G^0]$, tais que $G \models \forall x\, (\phi^0(xc_1^{-1}) \vee \ldots \vee \phi^0(xc_k^{-1}))$.

Sendo o mesmo verdade em G_1, um dos c_i satifaz $G_1 \models \phi^0(ac_i^{-1})$. Mas $g \in Stab(p)$ implica $t(ga/G) = t(a/G)$, donde $G_1 \models \phi^0(gac_i^{-1})$. Então $g \in G^0$.

QED

Proposição 5.2.3. Sempre $\mathrm{RM}(Stab(p)) = \mathrm{RM}(p)$.

Demonstração: Considere G_1 extensão elementar de G em que todos os seus 1-tipos são realizados. Seja p_1 o herdeiro de p sobre G_1.

Sabemos que $\mathrm{RM}(Stab(p))$ é o máximo dos postos $\mathrm{RM}(q)$ com $Stab(p) \in q$. Dado $q \in \langle Stab(p) \rangle \subseteq S_1(G)$, existe $b \in G_1$ tal que $q = t(b/G)$, ou seja, b satisfaz em G_1 a fórmula que define $Stab(p)$ em G; portanto, $b \in Stab(p_1)$. Então $b^{-1} \in Stab(p_1)$ e $b^{-1} \cdot p_1 = p_1$.

Seja a um elemento de uma extensão elementar de G_1 satisfazendo p_1. Então $b^{-1}a$ realiza $b^{-1} \cdot p_1 = p_1$, de modo que $t(b^{-1}a/G_1) = p_1$ e $t(b^{-1}a/G) = p$. Obtemos, é claro, $\mathrm{RM}(b^{-1}a/G) = \mathrm{RM}(p)$.

Mas a função de inversão $(\cdot)^{-1}$ é uma bijeção definível e todo conjunto definível D tem o mesmo posto que D^{-1}, enquanto $b^{-1}a \in D \Leftrightarrow a^{-1}b \in D^{-1}$. Assim, $\mathrm{RM}(a^{-1}b/G) = \mathrm{RM}(b^{-1}a/G)$. Como também o produto por a^{-1} é uma bijeção definível, concluímos que $\mathrm{RM}(b/G) = \mathrm{RM}(a^{-1}b/G) = \mathrm{RM}(p)$.

Assim, $\mathrm{RM}(q) = \mathrm{RM}(p)$, como desejado. QED

Para $p \in S_1(G)$, sempre $G \in p$ por ser o máximo de Def^1_G, donde $\mathrm{RM}(p) \leqslant \mathrm{RM}(G)$. Os tipos para os quais vale a igualdade têm propriedades especiais, que estudaremos nesta seção.

Definição 5.2.4. Um tipo $p \in S_1(G)$ é *genérico* se $\mathrm{RM}(p) = \mathrm{RM}(G)$.

Como veremos, os tipos genéricos são caracterizados pelo (i) posto, por definição; (ii) estabilizador com índice finito; (iii) estabilizador igual a G^0.

Lema 5.2.5. Tipos genéricos sempre existem, no máximo $\mathrm{dM}(G)$ (veremos no Corolário 5.2.11 que são realmente em número $\mathrm{dM}(G)$); o herdeiro de um tipo genérico é genérico; se p é genérico e $g \in G$, então $g \cdot p$ é genérico.

Demonstração: Para a primeira afirmação, temporária mas necessária, basta aplicar a Proposição 2.2.5. Se $G \prec G_1$, então $\mathrm{RM}(G) = \mathrm{RM}(G_1)$, de modo que um herdeiro tem mesmo posto. Finalmente, basta lembrar que $\mathrm{RM}(g \cdot p) = \mathrm{RM}(p)$. QED

Lema 5.2.6. Um tipo $p \in S_1(G)$ é genérico se e somente se $Stab(p)$ tem índice finito em G.

Demonstração: Se $Stab(p)$ tem índice finito, então $\mathrm{RM}(Stab(p)) = \mathrm{RM}(G)$, de modo que $\mathrm{RM}(p) = \mathrm{RM}(G)$ e p é genérico.

Assuma que p é genérico: como cada $g \cdot p$ é genérico, $[G : \mathit{Stab}(p)] = |\{g \cdot p \mid g \in G\}| \leqslant \mathrm{dM}(G)$. QED

Corolário 5.2.7. Um tipo $p \in S_1(G)$ é genérico se e somente se $\mathit{Stab}(p) = G^0$.

Demonstração: Lembramos que sempre $\mathit{Stab}(p) \subseteq G^0$. Se $\mathit{Stab}(p) = G^0$ então $\mathit{Stab}(p)$ tem índice finito e p é genérico. Se p é genérico, $\mathit{Stab}(p)$ tem índice finito e vem $G^0 \subseteq \mathit{Stab}(p)$. QED

Proposição 5.2.8. *G é conexo se e somente se $\mathrm{dM}(G) = 1$.*

Demonstração: Se G não é conexo, ou seja, existe um subgrupo H definível com $0 < [G : H] < \omega$, então $\mathrm{dM}(G) = \mathrm{dM}(H)\,[G : H] > 1$.

Assim, suponha G conexo com $\mathrm{RM}(G) = \xi$ e $\mathrm{dM}(G) = n$. Seja G_1 uma extensão elementar ω-saturada de G, com $\mathrm{RM}(G_1) = \xi$ e $\mathrm{dM}(G_1) = n$. Operaremos principalmente em G_1, que também é conexo por ser elementarmente equivalente a G.

Particione $G_1 = D_1 \cup \ldots \cup D_n$ com D_i definíveis, $\mathrm{RM}(D_i) = \xi$ e $\mathrm{dM}(D_i) = 1$. Seja ϕ_i a fórmula de $\mathrm{L}(G_1)$ que define D_i: sabemos que $\phi_i(g^{-1}v)$ define gD_i para $g \in G_1$.

Cada D_i determina $p_i \in S_1(G_1)$, genérico de G_1 com $\mathit{Stab}(p_i) = (G_1)^0 = G_1$. Assim, para qualquer $g \in G_1$, $g \cdot p_i = p_i$ e então $gD_i \in p_i$. Para $g_1, \ldots, g_k \in G_1$, temos $g_1D_i \cap \ldots \cap g_kD_i \in p_i$, sendo portanto um conjunto não-vazio. Existe então uma extensão elementar G_2 de G_1 em que $\bigcap_{g \in G_1} \phi_i(g^{-1}(G_2))$ não é vazia; seja $h \in G_2$ um elemento seu. Estendendo G_2 novamente se necessário, podemos supô-la ω-saturada, porque h ainda pertence à extensão e satisfaz as fórmulas $\phi_i(g^{-1}v)$.

Para todo $g \in G_1$, $h \in \phi_i(g^{-1}(G_2))$, donde $G_2 \models \phi_i[g^{-1}h]$ e então $g^{-1}h \in \phi_i(G_2)$. Concluímos que $g^{-1} \in \phi_i(G_2)h^{-1}$ e, substituindo g por $g^{-1} \in G_1$, $g \in \phi_i(G_2)h^{-1}$. Obtemos $G_1 \subseteq \phi_i(G_2)h^{-1}$.

Mas $\phi_i(G_2)h^{-1}$ é um definível com posto $\mathrm{RM}(\phi_i(G_2)) = \mathrm{RM}(D_i) = \xi$ e grau $\mathrm{dM}(\phi_i(G_2)) = \mathrm{dM}(D_i) = 1$. Pelo Lema 2.1.16 e sendo G_1, G_2 ω-saturadas, $\mathrm{dM}(G_1) \leqslant 1$ e obtemos $n = 1$. QED

Corolário 5.2.9. $\mathrm{dM}(G^0) = 1$ e $\mathrm{dM}(G) = [G : G^0]$.

Corolário 5.2.10. G é conexo se e somente se tem apenas um tipo genérico.

Demonstração: Pelas equações de posto, os tipos genéricos $p \in S_1(G)$ satisfazem $\mathrm{dM}(G) = \sum \mathrm{dM}(p)$, mas cada $\mathrm{dM}(p) = 1$. QED

Corolário 5.2.11. Há $\mathrm{dM}(G)$ tipos genéricos em $S_1(G)$ e quaisquer dois tipos genéricos têm mesma órbita pela ação $[\cdot]$.

Demonstração: Sendo p genérico, a cardinalidade de sua órbita é $[G : Stab(p)] = [G : G^0] = \text{dM}(G)$, que é o máximo de tipos genéricos, ou seja, o máximo é atingido. QED

Proposição 5.2.12. Sejam H um subgrupo definível e conexo de G e p seu tipo genérico. Então:

(i) Em uma extensão elementar $|G|^+$-saturada de G, qualquer elemento de H é o produto de duas realizações de p.

(ii) Se D é um subconjunto definível de H e $\text{RM}(D) = \text{RM}(H)$, então todo elemento de H é o produto de dois elementos de D, ou seja, $H = DD$.

Demonstração: (i) Suponha $h \in H$ e a uma realização de p em uma extensão elementar. Porque a é definível sobre ha^{-1} e reciprocamente, e $h \in G$, temos $\text{RM}(ha^{-1}/G) = \text{RM}(a/G)$. Assim, $t(ha^{-1}/G)$ é um tipo genérico de H, e é igual a p. Mas $h = ha^{-1}a$.

(ii) Já que o grau de H é 1, é impossível também $\text{RM}(H - D) = \text{RM}(H)$. Então a fórmula que define $H - X$ não está em p, de modo que p contém a fórmula que define D, digamos ϕ.

Para qualquer $h \in H$, portanto, a extensão elementar satisfaz $\exists u \exists v\, ((h = uv) \wedge \phi(u) \wedge \phi(v))$. Essa fórmula parametrizada vale, então, em G. QED

5.3. O teorema de indecomposição

Nesta seção, G é um grupo de posto de Morley *finito*.

Definição 5.3.1. Seja D um subconjunto definível de G. Dizemos que D é *indecomponível* se, para cada subgrupo definível H de G, o conjunto $D/H = \{Hg \mid g \in D\}$ é infinito ou unitário. ([Poizat 2] avisa que indecomponibilidade à esquerda e à direita não equivalem.)

Por definição, para todo subgrupo definível de G, ser conexo é o mesmo que ser indecomponível.

Proposição 5.3.2. Seja D um definível minimal de G. Então existe um indecomponível $D_0 \subseteq D$ tal que $D - D_0$ é finito.

Demonstração: Tome H_0 a intersecção dos subgrupos definíveis H de G tais que D/H é finito. Ora, então H_0 é intersecção de um número finito desses subgrupos, de modo que D/H_0 é finito. Já que D é minimal, um e apenas um dos conjuntos $H_0 g \cap D$, $g \in D$, é infinito e seu complemento em D é finito. Tome D_0 esse conjunto infinito e definível (é cofinito em D). Mostremos que D_0 é indecomponível.

Seja H um subgrupo definível de G. Se D/H é infinito, então D_0/H é infinito, pois $D - D_0$ é finito. Se D/H é finito, então $H_0 \subseteq H$ e D_0/H tem um único elemento. QED

Proposição 5.3.3. Seja D um subconjunto definível *normal* de G, isto é, $gDg^{-1} = D$ para todo $g \in G$. Então D é indecomponível se e somente se, para cada subgrupo definível *normal* N de G, o conjunto $D/N = \{Ng \mid g \in D\}$ é infinito ou unitário.

Demonstração: A implicação direta é dada pela definição. Suponha então que valha a propriedade a respeito dos subgrupos normais e seja H um subgrupo definível qualquer de G.

Para cada $g \in G$, a g-conjugação é uma bijeção que fixa D e leva H a gHg^{-1}, de modo que $|D/gHg^{-1}| = |D/H|$.

Tomando-se $N = \bigcap_{g \in G} gHg^{-1}$, existe um subconjunto finito G_0 de G tal que $N = \bigcap_{g \in G_0} gHg^{-1}$. Por sua definição, N é normal, e obtivemos N definível.

Vemos que, para $g \in G_0$, se $|D/N| = 1$ então $|D/gHg^{-1}| = 1|$ e se $|D/N| \geqslant \omega$ então $|D/gHg^{-1}| \geqslant \omega$. QED

Teorema 5.3.4 (Indecomposição de Zilber). Sejam D_i, $i \in I$, subconjuntos definíveis de G indecomponíveis, cada um contendo o elemento neutro 1 de G. Então o subgrupo gerado por $\bigcup_{i \in I} D_i$ é definível e conexo.

Demonstração: Acrescentando os conjuntos $D_i^{-1} = \{g^{-1} \mid g \in D_i\}$, $i \in I$, podemos supor que para cada i existe j tal que $D_i^{-1} = D_j$.

Seja H o subgrupo gerado por $\bigcup_{i \in I} D_i$.

Para cada seqüência finita $s = (i_1, \ldots, i_k)$ de elementos de I, considere o definível $D_s = D_{i_1} \ldots D_{i_k} = \{g_1 \ldots g_k \mid g_1 \in D_{i_1}, \ldots, g_k \in D_{i_k}\}$. Temos $D_s \subseteq H$. Como RM(G) é finito, existe uma seqüência t tal que RM(D_t) é máximo. Seja $p \in S_1(G)$ um tipo contendo D_t e com RM(p) = RM(D_t): basta tomar p determinado por um irredutível contido em D_t.

Mostraremos que $H = Stab(p)$.

Primeiramente, mostraremos que $D_i \subseteq Stab(p)$ para todo $i \in I$. Temos que $1 \in D_i$ implica $Stab(p) \in \{gStab(p) \mid g \in D_i\}$. Suponha que D_i não está contido em $Stab(p)$: então $Stab(p)$ não é o único elemento de $\{gStab(p) \mid g \in D_i\}$. Como D_i é indecomponível, existem $a_n \in D_i$ distintos, $n \in \mathbb{N}$, tais que se $n \neq n'$ então $a_n Stab(p) \neq a_{n'} Stab(p)$, donde $a_n \cdot p \neq a_{n'} \cdot p$. Então todos os tipos $a_n \cdot p$ têm posto RM(D_t) e contêm a fórmula que define o conjunto $D_i D_t$. Portanto, este conjunto tem posto estritamente maior que RM(D_t), contradição.

Assim, $H \subseteq Stab(p)$, o que implica $D_t \subseteq Stab(p)$. Mas RM($Stab(p)$) $\leqslant$ RM(p) = RM(D_t), donde RM(D_t) = RM($Stab(p)$). Sendo p um tipo genérico de $Stab(p)$, seu estabilizador em $Stab(p)$ é a componente conexa de $Stab(p)$, ou seja, $Stab(p)$ é conexo. Desse modo, $Stab(p) = D_t D_t$, donde $Stab(p) \subseteq H$.

QED

Exemplo 5.3.5. Assuma que G é conexo. Veremos que o grupo derivado G' gerado pelos comutadores $ghg^{-1}h^{-1}$, $g, h \in G$, é definível e conexo.

Para cada $g \in G$, tome $D_g = \{ghg^{-1}h^{-1} \mid h \in G\}$ definível e contendo 1. Então G' é gerado por $\bigcup_{g \in G} D_g$. Basta mostrar que cada D_g é indecomponível.

Tome $E_g = g^{-1}D_g = \{hg^{-1}h^{-1} | h \in G\}$. Para cada subgrupo N de G, temos $|D_g/N| = |E_g/N|$, pois a multiplicação por g^{-1} induz uma bijeção, bastando então mostrar que E_g é indecomponível. Suponha então N *normal*; devemos mostrar que $|E_g/N|$ é 1 ou infinita. Contudo, $hg^{-1}h^{-1}N = h'g^{-1}h'^{-1}N$ se e somente se Nhh'^{-1} pertence ao centralizador de Ng em G/N, de modo que $|E_g/N|$ é o índice desse centralizador. Não pode ser finito diferente de 1 porque G/N é conexo.

5.4. Grupos um-baseados

Nesta seção, suporemos que G é um grupo um-baseado com uma extensão elementar $\mathfrak{C}$, modelo monstro adequado.

Proposição 5.4.1. Se H é um subgrupo definível conexo de G, então o parâmetro canônico de H é algébrico sobre $\emptyset$.

Demonstração: Sejam g uma realização do tipo genérico de G, p o tipo genérico de H, p_1 o herdeiro de p sobre C e a uma realização de p_1. Seja $q = t(ga/C)$. Seja u o parâmetro canônico de H e v o de q.

Observamos que: por G ser um-baseado, v é algébrico sobre ga; $u \in G$; $t(ga/G)$ é um tipo genérico de G, donde ga e u são independentes sobre $\emptyset$; $\mathrm{RM}(q) = \mathrm{RM}(a/C) = \mathrm{RM}(H)$.

Mostraremos que u é definível sobre v. Assim, u é algébrico sobre ga e independente de ga sobre $\emptyset$, portanto algébrico sobre $\emptyset$. Provaremos que todo automorfismo de C fixando q fixa o subconjunto definido em C pela fórmula que define H.

Suponha ξ um automorfismo de $\mathfrak{C}$ com $\xi \cdot q = q$ e sejam $H_1 = \xi[H]$, $g_1 = \xi(g)$. Como $gH, g_1H_1 \in q$, temos $\mathrm{RM}(q) = \mathrm{RM}(H) \geqslant \mathrm{RM}(gH \cap g_1H_1) \geqslant \mathrm{RM}(q)$. Então $\mathrm{RM}(gH \cap g_1H_1) = \mathrm{RM}(H)$. Mas $gH \cap g_1H_1 = g_2(H \cap H_1)$ para qualquer $g_2 \in gH \cap g_1H_1$, donde $\mathrm{RM}(H \cap H_1) = \mathrm{RM}(H)$. Já que H é conexo, $H_1 = H$; já que $gH \cap g_1H_1 \neq \emptyset$, $gH = g_1H_1$. QED

Proposição 5.4.2. G é abeliano-por-finito, isto é, G tem um subgrupo abeliano definível de índice finito.

Demonstração: Provaremos que a componente conexa de G é abeliana; assumiremos então que G é conexo e mostraremos que é abeliano.

Considere, para $g \in G$, o subgrupo $H_g = \{(h, g^{-1}hg) \mid h \in G\}$ de G^2 e defina $g \sim g' \Leftrightarrow H_g = H_{g'}$. Como H_g é isomorfo a G, é conexo. Vemos também que $g \sim g'$ se e somente se $g'g^{-1}$ comuta com qualquer $h \in G$, de modo que a relação $\sim$ é definível. Como H_g é definível com parâmetros algébricos e conexo, existem, em qualquer extensão elementar de G, não mais que um número enumerável de grupos distintos da forma H_g, de modo que $\sim$ tem menos que ω classes, possível apenas se for um número finito de classes. A conclusão é que $Z(G)$ tem índice finito em G. QED

Proposição 5.4.3. Para todos $n \in \mathbb{N}$ e $p \in S_n(G)$, existe $g \in G$ tal que $gStab(p) \in p$.

Demonstração: Assumiremos $n = 1$ e que a base canônica de p é vazia — adicione os parâmetros necessários como constantes à linguagem. Sejam g uma realização do tipo genérico de G, p_1 o herdeiro de p sobre C e a uma realização de p_1. Seja $q = t(ga/C)$. Já que g é genérico e g e a são independentes sobre G, a e ga são independentes sobre G. Sejam S o estabilizador de p ou p_1, u o parâmetro canônico do definível gS e v a base canônica de q.

Primeiramente, mostraremos que u é definível sobre v e reciprocamente. Já que gS é definível com parâmetros em C, basta provar que, para cada automorfismo ξ de C, ξ fixa gS se e somente se fixa q. Mas $q = g \cdot p_1$, donde $\xi(q) = \xi(g) \cdot \xi(p_1) = \xi(g) \cdot p_1$, porque a base canônica de p_1 é vazia, de modo que $\xi(q) = q \Leftrightarrow g \cdot p_1 = \xi(g) \cdot p_1 \Leftrightarrow g^{-1}\xi(g) \in S \Leftrightarrow gS = \xi(g)S$. Mas $\xi[S] = S$, porque S é definível sem parâmetros: a base canônica de p é vazia. Assim, $\xi(q) = q \Leftrightarrow \xi[gS] = gS$.

Agora, como G é um-baseado, v é algébrico sobre ga, e u também é. Portanto, a e $ga \cup \{u\}$ são independentes sobre G, e a e ga são independentes sobre $G \cup \{u\}$. Seja $a_1 \in C$ realizando p e independente de u sobre G. Já que a base canônica de $q = t(ga/G)$ é definível sobre u, C e ga são independentes sobre $G \cup \{u\}$, a_1 e ga são independentes sobre $G \cup \{u\}$, e a_1 e $ga \cup \{u\}$ são independentes sobre G. Concluímos que $t((ga, u, a)/G) = t((ga, u, a_1)/G$. O fato de $ga \in gSa$ é expresso por uma fórmula com parâmetros ga, u (para definir gS) e a. Então $ga \in gSa_1$ e $a \in Sa_1$. Novamente, este fato pode ser expresso por uma fórmula com parâmetros a e a_1, já que S é definível sem parâmetros, então verdadeiro para quaisquer duas realizações independentes de p. Portanto, se b é uma realização de p em C, temos $a \in Sb$ e $bStab(p) \in p$. QED

Proposição 5.4.4. Para todo $n \in \mathbb{N}$, qualquer subconjunto definível de G^n

é uma combinação booleana finita de classes laterais de subgrupos definíveis conexos de G^n.

Demonstração: Note que, se H é um subgrupo definível, qualquer classe lateral de H é uma união finita de classes laterais da componente conexa de H. Podemos então ignorar a condição "conexos" no enunciado.

Para provar que qualquer fórmula é uma combinação booleana de fórmulas em uma família $\mathscr{F}$, basta mostrar que para quaisquer dois tipos distintos existe uma fórmula em $\mathscr{F}$ que pertence a apenas um deles.

Provaremos que $p = q$ se $p, q \in S_n(G)$ são tais que, para quaisquer subgrupo definível H de G e $g \in G$, vale $p \in Hg \Leftrightarrow q \in Hg$.

Assuma $\mathrm{RM}(q) \geqslant \mathrm{RM}(p)$. Sejam c, d realizações de p, q respectivamentem independentes sobre G. Seja $S = Stab(p)$. Sabemos que existe $g \in G$ tal que $c \in Sg$. Por hipótese, $d \in Sg$ e $dc^{-1} \in Sg$. Note que dc^{-1} e c são independentes sobre G. Temos $\mathrm{RM}(dc^{-1}/G \cup \{c\}) = \mathrm{RM}(d/G \cup \{c\}) = \mathrm{RM}(q) \geqslant \mathrm{RM}(p) \geqslant \mathrm{RM}(S)$, porque $\mathrm{RM}(Stab(p)) \leqslant \mathrm{RM}(p)$, e $\mathrm{RM}(S) \geqslant \mathrm{RM}(dc^{-1}/G)$, porque $dc^{-1} \in S$. Obtemos $q = t(d/G) = t(dc^{-1}c/G) = (dc^{-1}) \cdot p = p$. QED

5.5. Subgrupos fortemente minimais

Nesta seção, G é um grupo ω-estável *abeliano* de posto de Morley *finito*. [Lascar] informa que a hipótese de abelianidade é necessária somente em um momento e somente por simplicidade.

Proposição 5.5.1. Seja D um subconjunto definível fortemente minimal de G. Então existe um subgrupo definível conexo H de G tal que $H \subseteq \mathrm{acl}(D)$ e tal que $D - H$ é finito.

Demonstração: Tome D_0 indecomponível contido em D tal que $D - D_0$ é finito. Seja a um elemento de D_0 e tome $D_1 = a^{-1}D_0$. Então D_1 é indecomponível, contém 1 e está contido no fecho algébrico de D. Tome H o subgrupo gerado por G. É definível e conexo pelo Teorema da Indecomposição. Está contido no fecho algébrido de D e, como contém D_1, D/H é finito. QED

Seja D um subconjunto definível fortemente minimal de G. Considere a coleção $\mathscr{B}_D$ dos subgrupos conexos B de G, para cada um dos quais existe F finito tal que $B \subseteq \mathrm{acl}(F \cup D)$.

Já que o posto de G é finito, existe ao menos um elemento de $\mathscr{B}_D$ de posto maximal e maximal também quanto a inclusão. Além disso, se $B_1, B_2 \in \mathscr{B}_D$ então o subgrupo B_1B_2 gerado por $B_1 \cup B_2$ também está em $\mathscr{B}_D$. Então há um elemento máximo $B_D \in \mathscr{B}_D$. A proposição anterior afirma que D/B_D é finito.

Vemos também que, se D, E são subconjuntos definíveis fortemente minimais de G e não-ortogonais, então $B_D = B_E$.

Considere agora a a coleção $\mathscr{B}$ dos subgrupos conexos B de G, para cada um dos quais existem definíveis $D_1, \ldots D_n$ fortemente minimais e F finito tal que $B \subseteq \mathrm{acl}(F \cup D_1 \cup \ldots \cup D_n)$. Novamente, $\mathscr{B}$ tem um elemento máximo B; sejam $F, D_1, \ldots D_n$ para B. Então B contém B_D para todo fortemente minimal D.

Proposição 5.5.2. Existem definíveis fortemente minimais $D_1, \ldots, D_n$ dois a dois ortogonais tais que $B = B_{D_1} \ldots B_{D_n}$.

Demonstração: Considere a coleção dos subgrupos de G da forma $B_{E_1} \ldots B_{E_n}$ com E_i fortemente minimais. Pelo Teorema da Indecomposição, cada E_i é conexo e, como acima, existe um subgrupo máximo $H = B_{D_1} \ldots B_{D_n}$. Observamos que $H \subseteq B$ e que, para cada D fortemente minimal, $B_D \subseteq H$, de modo que D/H é finito. Esta propriedade se estende a qualquer conjunto de posto 1, porque pode ser particionado em um número finito de fortemente minimais.

Suponha que $H \neq B$. Então B/H é infinito e existe $c \in B$ tal que cH não é algébrica sobre F. Por outro lado, existe um conjunto finito $Y \subseteq D_1 \cup \ldots D_n$ tal que $c \in \mathrm{acl}(F \cup Y)$. Escolha Y minimal. Então $cH \in \mathrm{acl}(F \cup Y)$, existindo $Y' \subseteq Y$ e $y \in Y$ tais que $cH \in \mathrm{acl}(F \cup Y' \cup \{y\})$, mas $cH \notin \mathrm{acl}(F \cup Y')$. Tome $Y_0 = Y - \{y\}$, de modo que $c \notin \mathrm{acl}(F \cup Y_0)$ porque Y é minimal, $cH \in \mathrm{acl}(F \cup Y_0 \cup \{y\})$ e $c \in \mathrm{acl}(F \cup Y_0 \cup \{cH\})$.

Em particular, $\mathrm{RM}(c/F \cup Y_0) = 1$, ou seja, c está contido em um $F \cup Y_0$-definível T de posto 1. Já que $c \in \mathrm{acl}(F \cup Y_0 \cup \{cH\})$, existe uma fórmula $\phi(u, v)$ com parâmetros em $F \cup Y_0$ e $k \geqslant 1$ tais que $G \models \phi(c, cH)$ e existem $\leqslant k$ elementos x satisfazendo $\phi(x, cH)$ em G. Podemos assumir então que $G \models \phi(d, dH)$ e existem $\leqslant k$ elementos x satisfazendo $\phi(x, dH)$ em G, para cada $d \in T$, de modo que d é algébrico sobre $F \cup Y_0 \cup \{dH\}$. Mas $\{dH \mid d \in T\}$ é finito e isso contradiz T ser infinito.

Finalmente note que, por G ser abeliano, podemos supor os subgrupos B_{D_i} distintos, agrupando cada produto de elementos do mesmo subgrupo quando se gera um elemento de B. Desse modo, obtemos os conjuntos D_i dois a dois ortogonais. QED

5.6. Grupos definíveis

Sejam L uma linguagem e $\mathfrak{A}$ uma L-estrutura arbitrárias, de modo que L não necessariamente expande a linguagem dos grupos.

Já conhecemos a primeira parte desta definição:

Definição 5.6.1. Um *grupo definível* em $\mathfrak{A}$ é um subconjunto definível G de A^n com operações de produto e inversão e elemento neutro também definíveis, sendo a restrição de funções definíveis em todo A^n, com as quais G é grupo.

Um *grupo infinitamente definível* em $\mathfrak{A}$ é a interseccção $G = \bigcap_{i \in I} G_i$ de subconjuntos definíveis G_i de A^n, $i \in I$, com operações de produto e inversão e elemento neutro também definíveis, sendo a restrição de funções definíveis em todo A^n, com as quais G é grupo.

Lembramos que basta o produto ser definível, porque $y = x^{-1} \Leftrightarrow xy = 1$.

Supomos $\mathfrak{A}$ ω-estável. Usaremos a notação multiplicativa $.\,, {}^{-1}, 1$.

Teorema 5.6.2. Se G é um grupo infinitamente definível em $\mathfrak{A}$, então G é definível em $\mathfrak{A}$.

Demonstração: Observe que, como $G \neq \emptyset$, a coleção $\{G_i \mid i \in I\}$ que define G tem a propriedade da intersecção finita: podemos supor, portanto, que é um filtro em Def_A^n, estendendo-a se necessário. Sejam ϕ_i as fórmulas de $\mathrm{L}(C)$ que definem G_i, respectivamente.

Vemos que $\{\phi_i(u), \phi_i(v), \phi_i(w) \mid i \in I\}$ implica $u1 = 1u = u$, $u^{-1}u = uu^{-1} = 1$, $(u^{-1})^{-1} = u$ e $(uv)w = u(vw)$ quando u, v, w são substituídos por elementos de G — são as propriedades de grupo.

Pelo Teorema da Compacidade, existe um subconjunto finito de I, ou um único $i \in I$ já que supomos filtro, tal que $\phi_i(u) \wedge \phi_i(v) \wedge \phi_i(w)$ já implicam essas propriedades. Podemos assumir, substituindo $\phi_i(u)$ por $\phi_i(u) \wedge \phi_i(u^{-1})$, que $\phi_i(u)$ equivale a $\phi_i(u^{-1})$.

Seja X um conjunto finito contendo os parâmetros de ϕ_i e seja S o conjunto dos $p \in S_n(X)$ que contêm ϕ_i e $\mathrm{RM}(p) = \mathrm{RM}(\phi_i(\mathfrak{A}))$. Então S é finito e qualquer realização de qualquer elemento de S pertence a G.

Considere $H = \{h \in A \mid$ para todo $a \in A$ tal que $t(a/X) \in S$ e $a \mathop{\smile\!\!\!\!\!\mid}_A h$, $\mathfrak{A} \models \phi_i[ha]\}$. Mostraremos que $H = G$ e que H é definível.

Dado $h \in H$, seja $a \in A$ tal que $t(a/X) \in S$ e $a \mathop{\smile\!\!\!\!\!\mid}_A h$. Então $\mathrm{RM}(ha/X) \geqslant \mathrm{RM}(ha/X \cup h) = \mathrm{RM}(a/X \cup h) = \mathrm{RM}(a/X) = \mathrm{RM}(\phi_i(\mathfrak{A}))$, donde $ha \in G$ e $h = haa^{-1} \in G$.

Reciprocamente, se $g \in G$ e $a \in A$ é tal que $t(a/X) \in S$ e $a \mathop{\smile\!\!\!\!\!\mid}_A g$, temos $ga \in G$, de modo que $\mathfrak{A} \models \phi_i[ga]$ e vem $g \in H$.

Note que $H = \{h \in A \mid \phi_i(\mathfrak{A}) \subseteq_\alpha \phi_i(h(\cdot), \mathfrak{A})\}$ é definível. QED

5.7. Corpos totalmente transcendentais

Optamos por apresentar aqui a seção homônima de [Pillay A]. Trabalhamos na linguagem dos anéis com unidade (apenas).

Lema 5.7.1. Suponha que K é um corpo infinito e totalmente transcendental. Então K tem um único tipo genérico.

Demonstração: Fazemos uso do grupo aditivo de K, porque consideramos tipos sobre K. Suponha que K tem um subgrupo aditivo A próprio e de índice finito. Então, para todo $x \in K$, xA é também subgrupo aditivo de K e existem $x_1, \ldots, x_n \in K$ tais que $\bigcap_{x \in K} xA = x_1 A \cap \ldots \cap x_n A$. Mas essa intersecção também tem índice finito em K, e é um ideal, portanto igual a K, contradição. Obtemos $K = K^0$. QED

Teorema 5.7.2 (Macintyre). Todo corpo infinito e totalmente transcendental é algebricamente fechado.

Referência: O Teorema 5.7.7 de [Hodges]. Sua demonstração pode ser acompanhada pelo material que desenvolvemos.

Corolário 5.7.3. Toda teoria de corpos infinitos com eliminação de quantificadores nessa linguagem contém ACF.

Demonstração: Vimos que é a eliminação de quantificadores responsável pela forte minimalidade dos corpos algebricamente fechados, portanto por seu posto 1. Concluímos, de fato, que os únicos postos ordinais para corpos são 0 (corpos finitos) e 1 (corpos algebricamente fechados); os demais corpos têm "posto" ∞. QED

Variedades Algébricas

6
Um pouco de Geometria Algébrica

Como procedemos na primeira parte, descreveremos neste capítulo o assunto que trataremos, sem numerar definições. Observamos, contudo, que esta exposição é muito mais restrita e dirigida a nosso objetivo.

Introduções à Geometria Algébrica sem pré-requesitos específicos à área são [Hartshorne], [Shafarevich] e o início de [Lang 2], mas é necessário algum cuidado ao interpretar enunciados, porque as definições variam de texto para texto. Em particular, as variedades com que trabalhamos são sempre irredutíveis.

Trabalharemos sempre com um corpo K algebricamente fechado: embora as definições posteriores possam ser adaptadas para corpos arbitrários, raízes suficientes facilitam o trabalho. Quando considerarmos K^n ou $K[x_1, \ldots, x_n]$, assume-se $n \geqslant 1$.

Indicaremos um espaço topológico como seu próprio conjunto-base e, contrariamente à notação anterior de pré-geometrias, usaremos $\mathrm{cl}(\cdot)$ para indicar o fecho topológico. Uma função é fechada se a imagem de qualquer fechado é fechada.

6.1. Espaços noetherianos e a topologia de Zariski

Trabalharemos com topologias que incluam uma noção de dimensão. Os exemplos dos espaços afins $\mathbb{A}^n(K)$ e projetivos $\mathbb{P}^n(K)$, com que mais trabalharemos, são o início da Geometria Algébrica de variedades.

Um espaço topológico é *noetheriano* se não existe uma cadeia decrescente de subconjuntos fechados, ou seja, se toda cadeia descendente de fechados estaciona (em "comprimento" finito). Nesse caso, a intersecção de uma família de fechados é igual à intersecção de um número finito deles, como vimos na Proposição 5.1.4 para subgrupos definíveis. A topologia induzida em um subconjunto será também noetheriana.

Um conjunto não-vazio é dito *irredutível* se não é união de dois subconjuntos fechados (na topologia induzida) próprios. Apesar do nome, um irredutível pode conter outro. Note que o conceito de irredutibilidade implica e é mais restritivo que o de conexidade: por exemplo, na topologia usual de intervalos de $\mathbb{R}$, todo intervalo fechado é conexo, mas apenas os unitários são irredutíveis, como se vê na união $[a, c] = [a, b] + [b, c]$ para $a < b < c$. Duas componentes irredutíveis que se intersectam estam na mesma componente conexa.

O tratamento centra-se no conceito de irredutibilidade. Assim, caso usemos o de conexidade topológica, avisaremos explicitamente para não confundir com a conexidade de grupos.

Fato 6.1.1. Se F é um subconjunto fechado não-vazio de um espaço noetheriano, então existem fechados irredutíveis $F_1, \ldots, F_k$ tais que $F = F_1 \cup \ldots \cup F_k$ e cada F_i não está contido em nenhum outro F_j; *note que **não** são necessariamente dois a dois disjuntos.* Tais fechados (assim como k) são únicos, exceto por permutação, e chamados *componentes (irredutíveis) de F.*

Referências: A Proposição I.1.5 de [Hartshorne] ou o Teorema IX.2.2 de [Lang], embora se refira a fechados de Zariski.

Se X é um espaço topológico, existe o supremo ξ dos comprimentos ordinais ζ de cadeias de fechados irredutíveis $F_0 \subset F_1 \subset \ldots \subset F_\zeta$, em que todas as inclusões são próprias. Diz-se que X tem *dimensão* $\dim X = \xi$. A dimensão de um fechado é, por definição, sua dimensão como subespaço topológico.

Diretamente das definições, verifica-se o

Fato 6.1.2. (i) A dimensão de um fechado é o máximo dentre as dimensões de suas componentes. Se F é irredutível, então $\dim F = \sup\{\dim E + 1 \mid E$ é um fechado irredutível contido propriamente em $F\}$.

(ii) Se $E \subseteq F$ são fechados irredutíveis, então $\dim E \leqslant \dim F$, com igualdade se e somente se $E = F$.

(iii) Todo subconjunto aberto não-vazio de um conjunto irredutível é irredutível e denso nesse conjunto. Todo fecho de conjunto irredutível é irredutível.

Trabalharemos apenas com espaços com dimensão finita, o que é realmente uma hipótese importante além de simplificadora, mas este é um exemplo diverso oferecido por [Marker A]:

Exemplo 6.1.3. Dado um ordinal $\xi > 0$, podemos tomar como fechados em ξ os próprios ordinais $0 \leqslant \zeta \leqslant \xi$ — note que obtemos uma topologia, mas ***não*** se trata da topologia usual de intervalos. Novamente, a boa ordem dos ordinais garante que ξ é noetheriano, porque a intersecção de um conjunto de ordinais é seu *mínimo.* Nessa topologia, todo fechado não-vazio é irredutível. Vemos que $\dim(n) = n - 1$ para $1 \leqslant n < \omega$ e $\dim(\zeta) = \zeta$ para $\omega \leqslant \zeta \leqslant \xi$.

O nome "noetheriano" vem da condição homônima em Álgebra, que precisamos estudar brevemente. Considere o anel de polinômios $K[x_1, \ldots, x_n]$:

Teorema 6.1.4 (Base de Hilbert). Toda cadeia crescente de ideais estaciona (em "comprimento" finito) — diz-se que o anel é *noetheriano*; *observe a inversão das inclusões das cadeias* Em particular, todo ideal é finitamente gerado.

Referências: O início da Seção 7.9 de [Jacobson II] ou a Seção IV.4 e o início da Seção X.1 de [Lang].

Para qualquer $X \subseteq K^n$, defina $I(X)$ o conjunto desses polinômios que se anulam em todos os pontos de X: vemos que se trata de um ideal, chamado o *ideal* de X. Para qualquer $S \subseteq K[x_1, \ldots, x_n]$, defina $Z(S)$ o conjunto das raízes comuns aos polinômios em S, ou seja, os pontos de K^n que anulam todos os elementos de S, chamados *zeros* de S: esse conjunto também é indicado $V(S)$ em muitos textos.

Fato 6.1.5. Se I é o ideal gerado por $S \subseteq K[x_1, \ldots, x_n]$, então $Z(I) = Z(S)$.

Basta lembrar que I é o conjunto das somas $\sum_{i=1}^{k} p_i s_i$ com $k > 0$, $p_i \in K[x_1, \ldots, x_n]$ e $s_i \in S$.

K^n é chamado *espaço afim n-dimensional* sobre K e é tradicionalmente indicado $\mathbb{A}^n = \mathbb{A}^n(K)$. Um subconjunto *fechado (de Zariski) ou algébrico* de K^n é da forma

$$\bigcap_{1 \leqslant i \leqslant r} \{x \in K^n \mid f_i(x) = 0\} = Z(f_1, \ldots, f_r)$$

com $r \geqslant 1$ e $f_i \in K[x_1, \ldots, x_n]$. O fato de r ser finito permite-nos trabalhar com fórmulas e usar ferramentas modelo-teóricas, mas o que motiva a definição é o

Corolário 6.1.6. Qualquer conjunto de zeros $Z(S)$, para $S \subseteq K[x_1, \ldots, x_n]$, é fechado.

Demonstração: Seja I o ideal gerado por S em $K[x_1, \ldots, x_n]$. Pelo Teorema da Base de Hilbert, I é gerado por um número finito r de polinômios $f_1, \ldots, f_r$. Então $Z(S) = Z(I) = Z(f_1, \ldots, f_r)$. QED

Tanto para fins práticos como para desenvolver nossa intuição, apresentamos este lema tradicional:

Lema 6.1.7. Suponha $X, Y, X_j \subseteq K^n$ e $S, T, S_j \subseteq K[x_1, \ldots, x_n]$ para $j \in J$.

(i) Se $X \subseteq Y$ então $I(Y) \subseteq I(X)$; se $S \subseteq T$ então $Z(T) \subseteq Z(S)$.

(ii) $I\big(\bigcup_{j\in J} X_j\big) = \bigcap_{j\in J} I(X_j)$ e $Z\big(\bigcup_{j\in J} S_j\big) = \bigcap_{j\in J} Z(S_j)$. Note que, em *ambas* as igualdades, a união ocorre no argumento.

(iii) $Z(I(X))$ é o fecho de X. Veremos um enunciado correspondente a $I(\cdot)$ no Corolário 6.1.11.

Demonstração: As afirmações (i) e (ii) são derivadas das definições. Para (iii), seja $\mathrm{cl}(X)$ o fecho de X. Já que $X \subseteq Z(I(X))$ fechado, temos $\mathrm{cl}(X) \subseteq Z(I(X))$. Considere agora um fechado arbitrário V contendo X: então $V = Z(S)$ para algum conjunto de polinômios S que gera um ideal I. Vem $X \subseteq Z(I)$, donde $I(Z(I)) \subseteq I(X)$. Contudo, $I \subseteq I(Z(I))$ e então $Z(I(X)) \subseteq Z(I) = V$. Concluímos que $Z(I(X)) = \mathrm{cl}(X)$. QED

Como costumeiro, os complementos de conjuntos fechados são chamados *abertos*. Obtemos a

Proposição 6.1.8. Os abertos formam uma topologia sobre K^n, chamada *de Zariski*, com a qual K^n é noetheriano. *Atenção:* ***não*** *se trata da topologia homônima de* $\mathrm{Spec}\, K[x_1, \ldots, x_n]$ *apresentada no Exemplo 1.3.20.*

Demonstração: Trabalharemos diretamente com os fechados, que pelo corolário podemos supor como conjuntos de zeros de coleções arbitrárias de polinômios. Note que, tomando $0, 1 \in K[x_1, \ldots, x_n]$, temos $Z(1) = \emptyset$ e $Z(0) = K^n$.

Para concluir que a união finita de fechados é fechada, basta mostrá-lo para uma união de dois fechados. Suponha $S, T \subseteq K[x_1, \ldots, x_n]$ e considere o conjunto U dos polinômios fg com $f \in S$, $g \in T$. Ora, toda raiz comum dos polinômios de S é raiz dos polinômios de U, assim como os pontos de $Z(T)$. Reciprocamente, suponha $x \in Z(U)$, mas $x \notin Z(S)$. Seja $f \in S$ com $f(x) \neq 0$. Para todo $g \in T$, temos $(fg)(x) = 0$, donde $g(x) = 0$ e $x \in Z(T)$. Concluímos que $Z(S) \cup Z(T) = Z(U)$.

Devemos finalmente mostrar que a intersecção qualquer de fechados é fechada. Suponha $S_j \subseteq K[x_1, \ldots, x_n]$ para $j \in J$. Pela definição de $Z(\cdot)$, temos $\bigcap_{j \in J} Z(S_j) = Z\big(\bigcup_{j \in J} S_j\big)$ e este conjunto é fechado pelo corolário.

Se $F_0 \supseteq F_1 \supseteq \ldots$ é uma cadeia descrescente de fechados de K^n, então $I(F_0) \subseteq I(F_1) \subseteq \ldots$ é uma cadeia crescente de ideais, que estaciona em digamos $I(F_k)$. Como $F_i = Z(I(F_i))$, a cadeia de fechados também estaciona em F_k. QED

Um subconjunto do espaço topológico é *construtível* se for uma combinação booleana (finita) de fechados.

Teorema 6.1.9 (Tarski–Chevalley). (i) Os subconjuntos construtíveis de K^n na topologia de Zariski são precisamente os elementos de Def^n_K.

(ii) A imagem de um construtível por uma transformação com componentes polinomiais, isto é, $(f_1, \ldots, f_m)$ com cada $f_i \in K[x_1, \ldots, x_n]$, é construtível.

Em particular, os construtíveis são fechados sob qualquer tipo de projeção, que leva $(a_1, \ldots, a_n)$ a $(a_{i_1}, \ldots, a_{i_m})$.

Demonstração: (i) Os fechados de Zariski são conjuntos de raízes de um número finito de polinômios, de modo que todos os construtíveis são definíveis. Por outro lado, pela eliminação de quantificadores em ACF, todo definível pode ser definido por uma fórmula sem quantificadores, que é combinação booleana de fórmulas atômicas. Estas, por sua vez, sabemos que são da forma "polinômio $= 0$" (na linguagem dos anéis, por exemplo) e definem conjuntos fechados.

(ii) Basta observar que funções polinomiais são definíveis. QED

A recíproca está intimamente associada, porque basta remover um quantificador existencial por vez, começando pelos mais internos ou aninhados, sendo o quantificador universal apenas uma abreviatura. De fato, uma fórmula da forma $\exists v\, \phi$, com ϕ sem quantificadores, corresponde à projeção usual de uma combinação booleana finita de fechados, aqueles definidos pelas fórmulas atômicas de ϕ.

Antes de prosseguir, precisamos destacar a família importante de ideais radicais. Um ideal J de $K[x_1, \ldots, x_n]$ é chamado *ideal radical* se, para quaisquer $p \in K[x_1, \ldots, x_n]$ e $k > 0$ com $p^k \in j$, temos $p \in J$. É o caso de todo ideal primo.

Se I é um ideal arbitrário, tome $\sqrt{I} = \{p \in K[x_1, \ldots, x_n] \mid p^k \in I$ para algum $k > 0\}$, chamado o *radical de I*. Vemos que $I \subseteq \sqrt{I}$, com igualdade se e somente se o próprio I é radical. O Teorema 7.2 de [Jacobson II] ou o Corolário X.2.3 de [Lang] mostram que $\sqrt{I}$ é igual à intersecção de todos os ideais primos contendo I, portanto um ideal radical. Observamos que o radical é indicado nilrad em [Jacobson II] e rad em [Lang].

Teorema 6.1.10 (*Nullstellensatz* de Hilbert). Sejam I um ideal e p um polinômio de $K[x_1, \ldots, x_n]$. Suponha que todo $a \in K^n$ que seja raiz de todo polinômio em I é também raiz de p. Então $p \in \sqrt{I}$.

Referências: O Teorema IX.1.5 de [Lang] ou a seqüência ao Teorema 7.14 de [Jacobson II]. Algumas adaptações da prova de [Jacobson II] permitem apresentá-la em roupagem modelo-teórica: o Lema 2.3 de [Pillay A] ou o Teorema 3.2.11 de [Marker]. De fato, o *Nullstellensatz* equivale a este outro enunciado, mais modelo-teórico: "Suponha $f_1, \ldots, f_r, g_1, \ldots, g_s \in K[x_1, \ldots, x_n]$ tais que o sistema de equações e inequações

$$f_1(x) = 0, \ \ldots, \ f_r(x) = 0, \ g_1(x) \neq 0, \ \ldots, \ g_s(x) \neq 0$$

tenha uma solução em algum corpo extensão de K; então esse sistema já tem uma solução em K^n." Este é o Teorema 7.14 de [Jacobson II] (podemos reescrever $(g_1 \dots g_s)(x) \neq 0$) e facilmente demonstrável com a modelo-completude dos corpos algebricamente fechados, bastando tomar um fecho algébrico da extensão de K (o Exemplo 1 da Seção 8.1 de [Hodges] ou o Teorema 6.5 de [Poizat 1]). Aliás, vemos que a própria modelo-completude confunde-se com essa propriedade. A equivalência dos dois enunciados é indicada no Exercício 8.1.11 de [Hodges].

Corolário 6.1.11. Para $S \subseteq K[x_1, \dots, x_n]$, $I(Z(S))$ é o radical do ideal gerado por S.

Demonstração: Seja I o ideal gerado por S: temos $Z(I) = Z(S)$. O *Nullstellensatz* afirma que se $p(a) = 0$ para todo $a \in Z(I)$ então $p \in \sqrt{I}$, ou seja, $I(Z(I)) \subseteq \sqrt{I}$. Por outro lado, se $p \in \sqrt{I}$ então $p^k \in I$ para algum $k > 0$, de modo que se $a \in Z(I)$ então $(p(a))^k = 0$ ou simplesmente $p(a) = 0$, concluindo-se que $p \in I(Z(I))$ e, enfim, $\sqrt{I} \subseteq I(Z(I))$. QED

Corolário 6.1.12. As associações $I(\cdot)$ e $Z(\cdot)$ são funções bijetoras entre as famílias de fechados de K^n e de ideais radicais de $K[x_1, \dots, x_n]$, sendo uma inversa da outra. Por essa bijeção, os fechados irredutíveis correspondem precisamente aos ideais primos próprios, cujo conjunto é indicado $\operatorname{Spec} K[x_1, \dots, x_n]$.

Demonstração: O Lema 6.1.7 e o corolário anterior indicam que $I(\cdot)$ e $Z(\cdot)$ são uma inversa da outra entre as famílias mencionadas. Desse modo, aos fechados não-vazios correspondem precisamente os ideais radicais próprios, porque $I(\emptyset) = K[x_1, \dots, x_n]$.

Suponha primeiramente X fechado irredutível e $pq \in I(X)$. Então $X \subseteq Z(pq) = Z(p) \cup Z(q)$, donde $X = (X \cap Z(p)) \cup (X \cap Z(q))$ ambos fechados. Portanto, ou $X = X \cap Z(p)$ e $p \in I(X)$, ou $X = X \cap Z(q)$ e $q \in I(X)$. Concluímos que $I(X)$ é primo, próprio porque $X \neq \emptyset$.

Seja agora I um ideal primo próprio e suponha $Z(I) = X \cup Y$ fechados. Obtemos $I = I(X) \cap I(Y)$. Se $p \in I(X)$, mas $p \notin I$, e $q \in I(Y)$, mas $q \notin I$, temos $pq \in I(X) \cap I(Y) = I$, contradizendo o fato de I ser primo. Assim, $I = I(X)$ ou $I = I(Y)$, e então $Z(I) = X$ ou $Z(I) = Y$. Como I é próprio, temos $Z(I) \neq \emptyset$ e podemos declarar $Z(I)$ irredutível. QED

Por exemplo, o espaço $\mathbb{A}^n$ é irredutível, porque é gerado pelo polinômio nulo, cujo ideal é primo.

Além dos espaços afins $\mathbb{A}^n$, são muito importantes também os espaços projetivos, que agora definiremos.

Define-se em $K^{n+1} - \{(0, \dots, 0)\}$ esta relação de equivalência: x e y são identificados se existe $\lambda \in K^*$ tal que $x_i = \lambda y_i$ para todo $1 \leqslant i \leqslant n+1$.

O espaço quociente obtido é chamado *espaço projetivo n-dimensional* sobre K e é tradicionalmente indicado $\mathbb{P}^n = \mathbb{P}^n(K)$. Lidam-se com os pontos de $K^{n+1} - \{(0, \ldots, 0)\}$ como representantes de suas classes em $\mathbb{P}^n$: diz-se que x tem *coordenadas homogêneas* $(x_1 : \ldots : x_{n+1})$. Note que, se $x_i \neq 0$, todos os representantes dessa classe também têm i-ésima coordenada não-nula.

O espaço projetivo $\mathbb{P}^n$ corresponde ao conjunto de "retas pela origem" no espaço afim $\mathbb{A}^n$, sendo os coeficientes de uma "reta" não todos nulos. É também uma "compactificação" de $\mathbb{A}^n$, com um ponto "infinito" extra sob determinada associação: intuitivamente, $\mathbb{A}^1$ é uma reta e $\mathbb{P}^1$ é uma circunferência; $\mathbb{A}^2$ é um plano e $\mathbb{P}^2$ é uma superfície esférica.

Um polinômio com $n+1$ variáveis é *homogêneo* se, uma vez que se anule em $x \in K^{n+1}$, anula-se em quaisquer coordenadas homogêneas de x. A soma de dois tais polinômios e o produto de um por outro polinômio qualquer são também homogêneos, de modo que se pode considerar um ideal de polinômios homogêneos. São um caso particular os polinômios *homogêneos de grau n*, em que todos os monômios têm o mesmo grau n.

Considerando apenas polinômios homogêneos, novamente se definem os subconjuntos fechados de $\mathbb{P}^n$, que formam uma topologia com a mesma demonstração acima, mas no Corolário 6.1.6 toma-se I o ideal de polinômios homogêneos gerado por S. O radical de um ideal de polinômios homogêneos ainda tem seus elementos todos homogêneos, valendo portanto os análogos do Lema 6.1.7 e Corolários 6.1.11 e 6.1.12. Em particular, $\mathbb{P}^n$ é irredutível. Porque o Teorema da Base de Hilbert vale particularmente para esses ideais, o espaço $\mathbb{P}^n$ é noetheriano. Usaremos sempre, neste caso, $I(X)$ como o ideal dos polinômios *homogêneos*.

6.2. Definições

Estabeleceremos as categorias de variedades, ou seja, definiremos esses objetos e os morfismos entre eles, além de topologias e outras estruturas úteis. Adotamos uma abordagem minimalista inspirada em [Lang 2] e, em menor grau, [Hindry, Silverman]. Outras referências úteis são [Pillay A], [Hartshorne] e [Shafarevich], embora alertemos que há diferentes definições dos "mesmos" objetos. A exposição de [Hindry] inicia-se sobre o corpo $\mathbb{C}$ dos números complexos, cuja teoria é mais rica ao herdar resultados analíticos.

Variedades e pontos racionais

Uma *variedade afim* é um subconjunto fechado *irredutível* de K^n. É o caso (extremo) de $\mathbb{A}^n$.

Subconjuntos abertos não-vazios de variedades afins são chamados *variedades quase-afins* e têm a topologia induzida. Por exemplo, $\mathbb{A}^1 - \{0\}$ é a variedade quase-afim correspondendo à remoção do fechado definido por $x_1 = 0$. Também o *grupo linear geral* $\mathrm{GL}(n)$ das matrizes $n \times n$ invertíveis é uma variedade quase-afim, dada por $\mathrm{GL}(n) = \{(x_{ij}) \in \mathbb{A}^{n^2} \mid \det(x_{ij}) \neq 0\}$.

Um subconjunto fechado *irredutível* de $\mathbb{P}^n$ é uma *variedade projetiva*.

Subconjuntos abertos não-vazios de variedades projetivas são chamados *variedades quase-projetivas* e têm a topologia induzida.

Atenção: por ***variedade*** *entendemos variedade (quase-)afim ou (quase-)projetiva. Veremos no Corolário 6.3.9 como entender todas as variedades como variedades quase-projetivas e na Proposição 6.3.8 como definir variedades abstratas apenas com base em variedades afins e entender o espaço projetivo como uma tal.*

Lembramos que as variedades quase-afins e quase-projetivas, por terem a topologia induzida das variedades afins e projetivas que são irredutíveis, são elas próprias irredutíveis e seus fechos são as variedades afins e projetivas originais.

Trabalharemos sempre com subvariedades *fechadas e não-vazias*, ou seja, uma *subvariedade* é apenas um subconjunto fechado que preferimos destacar dos outros fechados.

Ao considerar um conjunto fechado, os subconjuntos fechados na topologia induzida já são fechados na topologia do espaço original. Desse modo, se V é uma variedade quase-afim, então existem polinômios $f_1, \ldots, f_r, g_1, \ldots, g_s$ com coeficientes em K tais que $V = Z(f_1, \ldots, f_r) - Z(g_1, \ldots, g_s)$, escrevendo-se uma identidade análoga para variedades quase-projetivas com polinômios homogêneos.

Se K_0 é um subcorpo de K e V é uma variedade qualquer, dizemos que V *está definida sobre* K_0 ou que K_0 *é um corpo de definição de* V se os polinômios que definem V podem ser escolhidos com coeficientes em K_0.

Suponha V uma variedade quase-afim. Se L é uma extensão ou um subcorpo de K sobre o qual V está definida como $V = Z(f_1, \ldots, f_r) - Z(g_1, \ldots, g_s)$, as raízes em L^n comuns a $f_1, \ldots, f_r$ mas não a $g_1, \ldots, g_s$ são chamadas *pontos racionais de* V *em* L ou *pontos* L*-racionais* e formam o conjunto $V(L) = Z_L(f_1, \ldots, f_r) - Z_L(g_1, \ldots, g_s)$. Então $V(K) = V$, mas a notação esclarece o contexto. No caso de V ser uma variedade quase-projetiva, procede-se analogamente quanto aos pontos agora em L^{n+1} e os polinômios agora homogêneos que definem V. Desse modo, podemos sempre trabalhar com um corpo qualquer, tomando as variedades em seu fecho algébrico.

A notação $V(L)$ é análoga à modelo-teórica $\phi(\mathfrak{A})$. Exploraremos essa relação na Seção 6.4, mostrando inicialmente que $V(L)$ independe, em qualquer caso, da escolha específica de $f_1, \ldots, f_r, g_1, \ldots, g_s$, desde que tenham coeficientes em L.

Funções regulares, corpos de funções e morfismos

Seguiremos aqui a exposição da Seção I.3 de [Hartshorne]. Lembramos que polinômios são funções quando valorados usualmente.

Suponha primeiramente V uma variedade quase-afim e X um aberto de V. Uma função $f : X \to K$ é *regular em* $x \in X$ se existem polinômios p, q com coeficientes em K tais que q não se anula em x e $f = p/q$ em toda uma vizinhança aberta de x, lembrando que o conjunto de pontos em que q não se anula é aberto pela definição da topologia de Zariski. A função é dita *regular (sobre* X*)* se o for em todo ponto de X.

Considere agora V uma variedade quase-projetiva e X um aberto de V. Uma função $f : X \to K$ é *regular em* $x \in X$ se existem polinômios p, q homogêneos de mesmo grau com coeficientes em K tais que q não se anula em x e $f = p/q$ em toda uma vizinhança aberta de x, lembrando novamente que o conjunto de pontos em que q não se anula é aberto. (Observe que p/q é uma função onde q não se anula porque p e q têm mesmo grau.) A função é dita *regular (sobre* X*)* se o for em todo ponto de X.

Vemos que as funções constantes são regulares.

Sendo V quase-afim ou quase-projetiva, define-se seu *corpo de funções* $K(V)$ como o conjunto das funções definidas em subconjuntos abertos de V e regulares em seus domínios, identificadas caso coincidam na intersecção de seus domínios. Observemos que $K(V)$ é de fato um corpo, definindo-se adição e multiplicação ponto a ponto (para obter inversos, novamente se usa o fato de que polinômios se anulam em fechados, restando um aberto) e é extensão de K quando se identificam $a \in K$ e a função constante a.

Há duas extensões de corpos muito importantes na Geometria Algébrica.

Um *corpo numérico* é uma extensão finita de $\mathbb{Q}$, então de característica 0.

Um *corpo de funções* é o corpo de funções de uma variedade sobre um corpo K_0, chamado *corpo constante*. Uma extensão K de K_0 é um corpo de funções sobre K_0 se e somente se satisfaz estas três condições: (i) K é finitamente gerado sobre K_0, (ii) todo elemento de K algébrico sobre K_0 já pertence a K_0, (iii) existem $t_1, \ldots, t_r \in K$ algebricamente independentes sobre K_0, tais que K é uma extensão separável finita de $K_0(t_1, \ldots, t_r)$.

Se V é uma variedade afim, o Teorema I.3.2(d) de [Hartshorne] caracteriza $K(V)$ de outro modo. Considere o anel $K[V]$, com operações definidas ponto a ponto, das funções de V em K dadas por polinômios de $K[x_1, \ldots, x_n]$. Temos $K[V] \cong K[x_1, \ldots, x_n]/I(V)$ e $K[V]$ é um domínio de integridade. Seu corpo de frações é isomorfo a $K(V)$.

Sejam V, W variedades definidas sobre K. Um *morfismo* $\phi : V \to W$ é uma função contínua tal que, para todo aberto $Y \subseteq W$ e toda função regular $f : Y \to K$, a função composta $f \circ \phi : \phi^{-1}[Y] \to K$ é regular. Por inspeção direta, verificamos que composição de morfismos é morfismo e funções constantes são morfismos. O morfismo é dito *isomorfismo* se for bijetor e sua inversa também for um morfismo.

Um morfismo de um subconjunto aberto não-vazio de V a W é chamado *função racional* de V a W. Caso a função racional $\phi : X \to W$, em que X é aberto de V, tenha uma inversa também racional $\psi : Y \to V$, com Y aberto de W, de modo que $\psi \circ \phi$ e $\phi \circ \psi$ sejam funções identidade, diz-se que ϕ é uma *função bi-racional* e que V e W são *bi-racionalmente equivalentes*.

Desse modo, um morfismo entre variedades afins pode ser visto como uma transformação com componentes polinomiais, globalmente agora.

Um morfismo entre variedades *está definido sobre* K_0 subcorpo de K, ou K_0 *é seu corpo de definição*, se os polinômios que formam suas componentes podem ser escolhidos com coeficientes em K_0.

Produtos de variedades

A bijeção natural entre $\mathbb{A}^m \times \mathbb{A}^n$ e $\mathbb{A}^{m+n}$ induz esta construção: se V, W são variedades afins em K^m, K^n respectivamente, também $V \times W$ é uma variedade afim. Primeiramente, é um subconjunto fechado de K^{m+n}: basta tomar simultaneamente os polinômios que definem V e W com variáveis $x_1, \ldots, x_m$ e $x_{m+1}, \ldots, x_{m+n}$ respectivamente. É também irredutível porque V e W são, como indicam os Exercícios I.3.15 e I.3.16 de [Hartshorne]. Do mesmo modo, o produto de variedades quase-afins é quase-afim. Note, porém, que a topologia de Zariski é mais fina que a topologia produto usual.

É preciso um pouco mais de atenção com espaços projetivos. Defina a *função de Segre* $S : \mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$,

$$S((x_1 : \ldots : x_{m+1}), (y_1 : \ldots : y_{n+1})) = ((x_i y_j)_{1 \leqslant j \leqslant n+1})_{1 \leqslant i \leqslant m+1} \,.$$

(Note que, nas coordenadas homogêneas, S tem domínio $K^{m+1} \times K^{n+1}$ e codomínio $K^{(m+1)(n+1)}$ e que independe das coordenadas em cada ponto.) Com essa função, define-se o *produto* de variedades (quase-)projetivas e vê-se que é uma variedade (quase-)projetiva.

Uma variedade V é *completa* se, para toda variedade W da mesma categoria, a projeção usual $\pi : V \times W \to W$ é fechada, isto é, leva fechados em fechados. Toda variedade projetiva é completa e toda função regular sobre uma variedade completa é constante.

Grupos algébricos

Um *grupo algébrico* é uma variedade V com morfismos $\mu : V \times V \to V$, em que o produto tem a topologia de Zariski, e $\rho : V \to V$ de modo que μ é uma operação de grupo sobre V e ρ é a operação de inversão correspondente. Note que, do modo que definimos, a variedade é sempre irredutível. Além disso, os grupos algébricos diferem dos grupos topológicos, em que se considera a topologia produto. Diz-se que o grupo algébrico *está definido* sobre um subcorpo K_0 se V, ρ e μ estão.

Dois exemplos importantes são o *grupo aditivo* $\mathbb{G}_a$, que é dado por $\mathbb{A}^1$ com a soma de K, e o *grupo multiplicativo* $\mathbb{G}_m$, que é dado por $\mathbb{A}^1 - \{0\}$ com a multiplicação de K, ou seja, K^*. Sabe-se que são os únicos grupos de dimensão 1. Também o grupo linear geral $\mathrm{GL}(n)$ é um grupo algébrico com o produto matricial usual. Sabe-se que todo grupo algébrico afim é um subgrupo de $\mathrm{GL}(n)$ para algum $n \in \mathbb{N}^*$.

Na maioria das situações, trabalharemos com grupos comutativos (abelianos), de modo que adotaremos a notação aditiva: elemento neutro 0, operação $+$ e inversão $-$. Por exemplo, o *transladado* de $X \subseteq G$ por $a \in G$ é o conjunto $a + X$ escrito aditivamente.

As subestruturas algébricas e geométricas de um grupo algébrico G são destacadas deste modo: um *subgrupo* de G é apenas um subconjunto contendo o elemento neutro e fechado sob as operações; uma *subvariedade* de G é apenas um subconjunto topologicamente fechado de G; um *subgrupo algébrico* de G é um subgrupo de G que é simultaneamente uma subvariedade, ou seja, um subgrupo fechado.

O mesmo se aplica às funções, que podem ser: um morfismo de variedades; um homomorfismo de grupos, que preserva o elemento neutro e as operações; um homomorfismo de grupos algébricos, que é simultaneamente um morfismo e preserva a estrutura algébrica.

Uma *variedade abeliana* é um grupo algébrico cuja variedade é completa. Atentamos para o fato de que o grupo é realmente abeliano ou comutativo, uma conseqüência de sua completude: veja o Exemplo 6.3.11.

O Lema 4.2 de [Pillay A] mostra que a variedade de um grupo algébrico é suave e separada, isto é, sua diagonal $\{(g,h) \in G^2 \mid g = h\}$ é fechada.

Um *toro (linear ou algébrico)* é um grupo algébrico isomorfo a um produto (finito) $\mathbb{G}_m \times \ldots \times \mathbb{G}_m$. Uma *variedade semi-abeliana* é um grupo algébrico S com subgrupo algébrico T que é um toro e S/T é variedade abeliana — para a definição de quociente, veja comentário na pág. 88 de [Poizat 2] e o Teorema A na Seção III.3 de [Shafarevich]. Um tal grupo é comutativo e divisível, isto é, para quaisquer $x \in S$ e $n \in \mathbb{N}^*$, existe $y \in S$ tal que $ny = x$.

Aproveitamos para recordar que, dado um grupo G, seu subgrupo $\{g \in G \mid ng = 0$ para algum $n \in \mathbb{N}^*\}$ é chamado *subgrupo de torsão* e, dado $n \in \mathbb{N}^*$, o subgrupo $\{g \in G \mid mg = 0$ para algum $m|n\}$ é chamado *subgrupo de n-torsão*

Para esta definição, podemos supor G um grupo arbitrário, embora tenhamos que mencionar a característica de K porque usaremos a definição para grupos algébricos. Suponha que G_0 é um subgrupo finitamente gerado de G. Se a característica de K é 0, suponha ainda que, para cada elemento $g \in G$, existe $n \in \mathbb{N}^*$ tal que $ng \in G_0$. Se a característica de K é $p > 0$, suponha ainda que, para cada elemento $g \in G$, existe $n \in \mathbb{N}^*$ que não é divisível por p e tal que $ng \in G_0$. Então dizemos que G tem *gradação finita*. (Em inglês, diz-se *finite rank*, mas [MTAG] alerta que não se trata do posto (*rank*) de Morley.)

Sem maiores detalhes, mencionamos a formulação tensorial desse conceito. Para característica 0, existe $r \in \mathbb{N}^*$ tal que $G \otimes \mathbb{Q} \cong \mathbb{Q}^r$. Para característica $p > 0$, existe $r \in \mathbb{N}^*$ tal que $G \otimes \mathbb{Z}_{(p)} \cong \mathbb{Z}_{(p)}^r$, em que $\mathbb{Z}_{(p)} = \{\frac{a}{p^k} \mid a \in \mathbb{Z}, k \in \mathbb{N}\}$.

Dimensão e suavidade

A *dimensão* de uma variedade V é $\dim V = k$ o comprimento máximo de uma cadeia de subvariedades irredutíveis $V_0 \subset \ldots \subset V_k = V$ em que todas as inclusões são próprias. Trata-se, portanto, da mesma dimensão definida para espaços noetherianos irredutíveis em geral. Note que, por maximalidade, V_0 é um conjunto unitário $\{(a_1, \ldots, a_n)\} = Z(x_1 - a_1, \ldots, x_n - a_n)$.

Obtemos a maximalidade da cadeia de ideais primos $I(V) = I(V_k) \subset \ldots \subset I(V_0) \subset K[x_1, \ldots, x_n]$. Lembramos também que $K[V] \cong K[x_1, \ldots, x_n]/I(V)$, estando os ideais em correspondência: $\dim V$ é também a *dimensão de Krull* do anel $K[V]$, que é simplesmente o comprimento máximo k de cadeias de ideais primos próprios $\{0\} = P_k \subset \ldots \subset P_0 \subset K[V]$ em que todas as inclusões são próprias. Equivalentemente, $\dim V$ é o grau de transcendência de seu corpo de funções $K(V)$ sobre K.

A dimensão é sempre um número natural (finito) e calcula-se $\dim \mathbb{A}^n = \dim \mathbb{P}^n = n$ pelo grau de transcendência.

Veremos, no Teorema 6.4.3, que $\dim V = \mathrm{RM}(V)$ quando V é uma variedade afim.

Agora, apresentamos o espaço tangente em um ponto, remetendo o leitor às Seções I.5 de [Hartshorne], A.1.4 de [Hindry, Silverman] e II.1 de [Shafarevich] para uma discussão completa.

Suponha que $V \subseteq K^n$ é uma variedade afim $V = Z(f_1, \ldots, f_r)$ definida por $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$, e suponha $a = (a_1, \ldots, a_n) \in V$. Lembramos que podemos derivar polinômios sem recurso a limites, de modo que se escrevem as equações $\sum_{i=1}^{n} \frac{\partial f_j}{\partial x_i}(a)(x_i - a_i) = 0$ para $1 \leqslant j \leqslant r$. O conjunto $T_a(V)$ das soluções simultâneas dessas equações em K^n é o *espaço tangente a V em a*. Esse conjunto é a soma de a com um subespaço vetorial de K^n, cuja dimensão então escrevemos $\dim T_a(V)$. Sabe-se que $T_a(V)$ independe dos polinômios $f_1, \dots, f_r$.

Para uma variedade V arbitrária, o espaço tangente é generalizado como um espaço dual. Sabe-se que, então, $\dim T_a(V) \geqslant \dim V$ para todo $a \in V$ e existe um subconjunto aberto próprio $X \subset V$ tal que $\dim T_a(V) = \dim V$ para todo $a \in X$. A esse respeito, conulte o Teorema I.5.3 de [Hartshorne] ou o Teorema 3 da Seção II.1 de [Shafarevich].

Os pontos para os quais vale a igualdade das dimensões da variedade e do espaço tangente são chamados *não-singulares* ou *suaves*. A variedade é também chamada *não-singular* ou *suave* se todos os seus pontos são não-singulares.

Novamente, quando $V = Z(f_1, \dots, f_r)$ é uma variedade afim e $a = (a_1, \dots, a_n) \in V$, o ponto a é suave se e somente se a matriz $\left(\frac{\partial f_j}{\partial x_i}(a)\right)$ tem posto $n - \dim V$.

Suavidade também pode ser caracterizada por propriedades algébricas de anéis *locais*, como na Seção I.5 de [Hartshorne] e na Seção II.1 de [Shafarevich].

Curvas e *genus*

Curvas são variedades de dimensão 1. Uma variedade abeliana de dimensão 1 é chamada *curva elíptica*. Toda curva é bi-racionalmente equivalente a uma única (a menos de isomorfismo) curva projetiva suave, como nota o Teorema A.4.1.4 de [Hindry, Silverman]. Assim, trabalharemos apenas com curvas projetivas suaves.

A cada curva associa-se um número natural chamado *genus*, cuja importância reside em sua invariância por funções bi-racionais. Não temos aqui nem as ferramentas nem o espaço necessários para definir esse número, de modo que nos satisfaremos em descrever suas propriedades importantes e referimos o leitor às Seções A.4.2 de [Hindry, Silverman] e I.2 de [Lang 2] para definições apropriadas.

Para introduzir o *genus*, [Hindry] atenta para o fato de que curvas sobre o corpo $\mathbb{C}$ são usualmente chamadas *superfícies de Riemann*. Intuitivamente, identificamos "alças" nesses objetos: uma esfera não tem alça; um toro tem uma alça; um bitoro tem duas alças. Nesse caso, o *genus* é precisamente o número de tais alças.

Também podemos mencionar que uma curva projetiva suave definida em $\mathbb{P}^2$ (plano) por um polinômio homogêneo de grau n tem *genus* $(n-1)(n-2)/2$. Veja o Teorema A.4.2.6 de [Hindry, Silverman] ou as p. 171–173 de [Shafarevich].

As curvas de *genus* 0 são bem conhecidas. De fato, lembramos que uma *cônica* é uma curva definida por um polinômio de grau 2. Sabe-se (o Teorema

A.4.3.1 de [Hindry, Silverman]) que cada curva suave projetiva de *genus* 0 é isomorfa a uma cônica em $\mathbb{P}^2$, e é isomorfa a $\mathbb{P}^1$ sobre um subcorpo K_0 se e somente se tem um ponto K_0-racional.

A família das curvas de *genus* 1 é muito mais rica. Entretanto, o Teorema A.4.4.1 de [Hindry, Silverman] mostra que uma curva de *genus* 1 é isomorfa a uma curva cúbica em $\mathbb{P}^2$.

As curvas com *genus* $\geqslant 2$ são, como se poderia intuir, ainda mais diversas, e os teoremas que buscam estudá-las tornam-se mais refinados e de demonstração mais elaborada. É o caso, por exemplo, da própria Conjectura de Mordell–Lang.

6.3. Resultados necessários

Esta seção relaciona alguns fatos de Geometria Algébrica, nem sempre básicos, necessários para o desenvolvimento de nosso raciocínio ou mesmo de nossa compreensão. Expomos uma fração do conteúdo de [Pillay A] e [Pillay B].

Considere ainda K algebricamente fechado e K_0 subcorpo de K.

Começamos por trabalhar os grupos algébricos. Seja G um grupo algébrico, não necessariamente comutativo, mas que indicaremos aditivo. Por definição, morfismos são contínuos; $+$, $-$ e funções constantes são morfismos e composta de morfismos é morfismo.

Vemos que, na topologia de Zariski em $\mathbb{A}^n$ ou $\mathbb{P}^n$, vê-se que transladado de aberto/fechado é aberto/fechado (para fechados pela definição, para abertos por complemento).

Lema 6.3.1. Suponha $a \in G$ e $X \subseteq G$. Definem-se $a+X = \{a+x \in G | x \in X\}$, $X + a = \{x + a \in G \mid x \in X\}$ e $-X = \{-x \in G \mid x \in X\}$. Então:

(i) Se X é fechado ou aberto, então $a + X$, $X + a$ e $-X$ são fechados ou abertos respectivamente.

(ii) $\mathrm{cl}(a + X) = a + \mathrm{cl}(X)$, $\mathrm{cl}(X + a) = \mathrm{cl}(X) + a$ e $\mathrm{cl}(-X) = -\mathrm{cl}(X)$.

Demonstração: Para verificar (i), defina as funções $\varphi_1 : G \to G$, $\varphi_1(g) = (-a) + g$; $\varphi_2 : G \to G$, $\varphi_2(g) = g - a$; e $\varphi_3 : G \to G$, $\varphi_3(g) = -g$; que sabemos serem contínuas. Temos $a + X = \varphi_1^{-1}[X]$; $X + a = \varphi_2^{-1}[X]$; e $-X = \varphi_3^{-1}[X]$.

Demonstremos (ii). Já que $X \subseteq \mathrm{cl}(X)$, temos $a + X \subseteq a + \mathrm{cl}(X)$ fechado por (i), de modo que $\mathrm{cl}(a+X) \subseteq a+\mathrm{cl}(X)$. Assim, também temos $a+\mathrm{cl}(X) = a + \mathrm{cl}((-a) + a + X) \subseteq a + (-a) + \mathrm{cl}(a + X) = \mathrm{cl}(a + X)$ e concluímos que $\mathrm{cl}(a + X) = a + \mathrm{cl}(X)$. Analogamente, obtemos $\mathrm{cl}(X + a) = \mathrm{cl}(X) + a$. De $X \subseteq \mathrm{cl}(X)$ vem $-X \subseteq -\mathrm{cl}(X)$ fechado por (i), donde $\mathrm{cl}(-X) \subseteq -\mathrm{cl}(X)$. Assim, $\mathrm{cl}(X) = \mathrm{cl}(-(-X)) \subseteq -\mathrm{cl}(-X) \subseteq -(-\mathrm{cl}(X)) = \mathrm{cl}(X)$, concluindo-se que $\mathrm{cl}(-X) = -\mathrm{cl}(X)$. QED

Lema 6.3.2. O fecho de um subgrupo de G é também um subgrupo de G (portanto, subgrupo algébrico).

Demonstração: Seja H subgrupo de G. Temos $\emptyset \neq H \subseteq \mathrm{cl}(H)$. Para todo $b \in H$, temos $H - b \subseteq H$, donde $\mathrm{cl}(H - b) \subseteq \mathrm{cl}(H)$ e, pelo lema anterior, $\mathrm{cl}(H) - b \subseteq \mathrm{cl}(H)$. Portanto, sendo $F = \{b \in G \mid \mathrm{cl}(H) - b \subseteq \mathrm{cl}(H)\}$,

$$H \subseteq F = \bigcap_{x \in \mathrm{cl}(H)} \{b \in G \mid x - b \in \mathrm{cl}(H)\} = \bigcap_{x \in \mathrm{cl}(H)} (-\mathrm{cl}(H) + x) .$$

Mas $-\mathrm{cl}(H) + x = \mathrm{cl}(-H + x)$ pelo lema anterior, de modo que F é fechado e contém $\mathrm{cl}(H)$. Assim, dados $a, b \in \mathrm{cl}(H)$, vem $a - b \subseteq \mathrm{cl}(H)$, como desejado.

QED

Proposição 6.3.3. Suponha X um subconjunto fechado, ou seja, uma subvariedade de G, e H um subgrupo de G. Então $X \cap H$ é uma união finita de transladados de subgrupos de G se e somente $X \cap H$ está contido em uma união finita, contida em X, de transladados de subgrupos algébricos de G.

Demonstração: Assuma que $X \cap H = \bigcup_{i=1}^{n}(a_i + H_i)$ com $a_i \in G$ e H_i subgrupos de G. Como X é fechado, $X \cap H \subseteq \mathrm{cl}(X \cap H) \subseteq X$, porém $\mathrm{cl}(X \cap H) = \bigcup_{i=1}^{n}(a_i + \mathrm{cl}(H_i))$ e cada $\mathrm{cl}(H_i)$ é, pelo lema anterior, subgrupo algébrico.

Assuma agora que $X \cap H \subseteq \bigcup_{i=1}^{n}(a_i + X_i) \subseteq X$ com $a_i \in G$ e X_i subgrupos algébricos de G. Temos $X \cap H = \bigcup_{i=1}^{n}(a_i + X_i) \cap H$. Se $(a_i + X_i) \cap H = \emptyset$, não é preciso considerar esse fator, que afinal não contribui para a união. Suponha então $b_i \in (a_i + X_i) \cap H$: mostraremos que $(a_i + X_i) \cap H = b_i + (X_i \cap H)$, o que conclui a demonstração porque $X_i \cap H$ são subgrupos de G.

Dado $y \in (a_i + X_i) \cap H$, temos $y = a_i + x$ com $x \in X_i$ e $y \in H$. Tome $x' = (-b_i) + a_i + x$: como $(-a_i) + b_i \in X_i$ e X_i é subgrupo, temos $(-b_i) + a_i \in X_i$, donde $x' \in X_i$; como $a_i + x = y \in H$ e $b_i \in H$ e H é subgrupo, temos $x' \in H$. Então $y = a_i + x = b_i + x' \in b_i + (X_i \cap H)$.

Dado $y \in b_i + (X_i \cap H)$, temos $y = b_i + x'$ com $x' \in X_i \cap H$. Tome $x = (-a_i) + b_i + x'$: como $(-a_i) + b_i \in X_i$ e $x' \in X_i$, temos $x \in X_i$. Então $a_i + x = b_i + x' = y$ e $y \in a_i + X_i$. Também $b_i, x' \in H$, donde $y \in H$ e $y \in (a_i + X_i) \cap H$.

Note que não foi necessária a hipótese de cada X_i ser fechado. QED

Corolário 6.3.4. Vemos que, na implicação direta, podemos tomar $\mathrm{cl}(X \cap H)$ como a união finita dos transladados de subgrupos algébricos. Essa é uma terceira formulação equivalente.

Depois dessa "exercitação", enunciamos alguns teoremas avançados:

Teorema 6.3.5 (Mordell–Weil). Se A é uma variedade abeliana sobre um corpo de números K, então $A(K)$ é um grupo finitamente gerado.

Referências: A Parte C de [Hindry, Silverman] ou o Capítulo 6 de [Lang 1], em que basta que K seja extensão finitamente gerada de seu corpo primo. Este texto também apresenta o caso de corpos de funções, conhecido como Teorema de Lang–Néron.

Teorema 6.3.6 (Jacobiana). Toda curva projetiva suave C de *genus* $g \geqslant 1$ definida sobre um subcorpo K_0 está imersa em uma variedade abeliana de dimensão g também definida sobre K_0, chamada a *variedade jacobiana de* C e indicada $J(C)$.

Referência: O Teorema A.8.1.1 de [Hindry, Silverman].

Teorema 6.3.7. Sejam V uma variedade suave e $X, Y \subseteq V$ variedades com $X \cap Y \neq \emptyset$. Então toda componente irredutível de $X \cap Y$ tem dimensão $\geqslant \dim X + \dim Y - \dim V$.

Referências: A demonstração é roteirizada a partir de exemplos na Seção 7 de [Marker A]. Veja também a Proposição I.7.1 e o Teorema I.7.2 de [Hartshorne] ou os Teoremas A.1.3.5 e A.1.3.6 de [Hindry, Silverman].

Introduziremos agora o conceito de variedade abstrata, que permite considerar apenas variedades afins em muitas aplicações. De fato, esta é a abordagem de [MTAG], mais especificamente das Seções 2 e 3 de [Pillay A].

Uma *variedade (abstrata)* é um conjunto $V = V_1 \cup \ldots \cup V_m$ com bijeções $f_i : V_i \to U_i$ onde U_i são variedades afins, $U_{ij} = f_i[V_i \cap V_j]$ são abertos de U_i e $f_j \circ f_i^{-1}$ são isomorfismos entre U_{ij} e U_{ji} como variedades quase-afins. A topologia é dada por: $U \subseteq V$ é aberto se, para todo i, $f_i[U \cap V_i]$ é aberto em U_i. Escrevemos $V = (V_i, f_i)_{1 \leqslant i \leqslant m}$.

Podemos então considerar V interpretável em K (ou definível em K^{eq}), do seguinte modo. Tome a união disjunta dos U_i com a relação de equivalência que identifique cada U_{ij} com U_{ji} via $f_j \circ f_i^{-1}$. Por eliminação de imaginários, obtemos V definível em uma potência de K, embora percamos a geometria.

Sejam, então, $V = (V_i, f_i)_{1 \leqslant i \leqslant m}$ e $W = (W_j, g_j)_{1 \leqslant j \leqslant n}$ variedades quaisquer. Uma função contínua $f : V \to W$ é um *morfismo* se, para todos i, j, a função $g_j \circ f \circ f_i^{-1}$ é um morfismo de variedades quase-afins. Novamente, um morfismo pode ser identificado com uma função definível entre os definíveis correspondentes às variáveis.

Não definiremos $V(L)$ formalmente: observamos apenas que se trata de "suspender" os pontos racionais das cartas afins.

Novamente, chama-se V *irredutível* se não tem dois subconjuntos fechados disjuntos e próprios cuja união seja V, isto é, V é conexa. Nesse caso, uma função *racional* de V a K é um morfismo de algum aberto de V a K. Identificamos funções racionais que coincidem na intersecção de seus domínios. Desse modo, o conjunto de funções racionais sobre V é o *corpo de funções* $K(V)$ de V.

Uma função *racional* ϕ de V a W é formada por $\phi_1, \ldots, \phi_n \in K(V)$ tais que $\phi(x) = (\phi_1(x), \ldots, \phi_n(x)) \in W$ para cada $x \in V$ em que todas as ϕ_j sejam racionais. É chamada *isomorfismo bi-racional* se existe outra função racional ψ de W a V tal que $(\phi \circ \psi)(y) = y$ e $(\psi \circ \phi)(x) = x$ para todos $x \in V$, $y \in W$ em que se definem.

O produto de V e W é a variedade

$$V \times W = (V_i \times W_j, (f_i, g_j))_{1 \leqslant i \leqslant m \text{ e } 1 \leqslant j \leqslant n}$$

em que $(f_i, g_j)(x, y) = (f_i(x), g_j(y))$ como usual.

Uma variedade V é *completa* se, para toda variedade W, a projeção usual $\pi : V \times W \to W$ é fechada, isto é, leva fechados em fechados.

Usaremos a

Proposição 6.3.8. Para cada $1 \leqslant i \leqslant n+1$, tome $A_i^n = \{(x_1 : \ldots : x_{n+1}) \in \mathbb{P}^n \mid x_i \neq 0\}$. Então $\mathbb{P}^n = A_1^n \cup \ldots \cup A_{n+1}^n$. Tome $f_i : A_i^n \to K^n$ bijeção dada por

$$f_i(x_1 : \ldots : x_{n+1}) = \left(\frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_{n+1}}{x_i}\right).$$

Então $(A_i^n, f_i)_{1 \leqslant i \leqslant n+1}$ é uma variedade definida sobre o corpo primo de K. $\mathbb{P}^n$ é interpretável sobre $\emptyset$ em K^{eq}, em bijeção $\emptyset$-definível com o conjunto $\emptyset$-definível correspondendo à variedade. Também $\mathbb{P}^n$ é bi-racionalmente isomorfo a $\mathbb{A}^n$ porque K é algebricamente fechado.

Temos $K(V) = K(V \cap A_1^n) = \ldots = K(V \cap A_{n+1}^n)$.

Corolário 6.3.9. Toda variedade quase-afim é quase-projetiva.

Demonstração: Se $X \subseteq \mathbb{A}^n$ então $Y = f_i^{-1}[X] \subseteq \mathbb{P}^n$. Seja Z o fecho de Y em $\mathbb{P}^n$. Temos $Y = Z \cap A_i^n$. QED

Concluímos com o

Teorema 6.3.10 (Rigidez). Suponha X, Y, Z variedades irredutíveis e $f : X \times Y \to Z$ um morfismo, de modo que X é completa e existe $y_0 \in Y$ tal que $f[X \times \{y_0\}]$ é um conjunto unitário. Então, para qualquer $y \in Y$, também $f[X \times \{y\}]$ é unitário, ou seja, a função f depende apenas de seu segundo argumento.

Referência: O Lema 3.18 de [Pillay A].

Exemplo 6.3.11. Este é o Exemplo 4.6 de [Pillay A]. A primeira tarefa é mostrar que uma variedade abeliana A é, de fato, um grupo comutativo. Considere o morfismo $f : A \times A \to A$, $f(x,y) = -x + y + x$. Temos $f[A \times \{0\}] = \{0\}$ e, portanto, para todo $y \in A$, vale $f[A \times \{y\}] = \{f_y\}$. Como $f(0,y) = y$, obtemos $f_y = y$ e, para todo $x \in A$, $-x + y + x = y$ ou $y + x = x + y$ como desejado.

Suponha agora que H é um outro grupo algébrico comutativo e $g : A \to H$ é um morfismo. Defina $g_1 : A \times A \to H$, $g_1(x,y) = g(x) + g(y) - g(x+y)$. Então $g_1(0,y) = g(0) = g_1(x,0)$ para quaisquer $x, y \in A$; aplicando-se o teorema duas vezes, $g_1(x,y) = g(0)$ para quaisquer $x, y \in A$. Assim, $g - g(0)$ é um homomorfismo de grupos algébricos e g é seu transladado.

6.4. Relações com a Teoria dos Modelos

É momento de compararmos a geometria modelo-teórica, que desenvolvemos na primeira parte, e a geometria das noções que definimos acima. Seja ainda K um corpo algebricamente fechado.

Já vimos que, se V é uma variedade quase-afim, existem polinômios $f_1, \ldots, f_r, g_1, \ldots, g_s$ com coeficientes em K tais que $V = Z(f_1, \ldots, f_r) - Z(g_1, \ldots, g_s)$, escrevendo-se uma identidade análoga para variedades quase-projetivas. No caso projetivo, não precisamos trabalhar com a identificação dos pontos de K^{n+1} e a interpretação modelo-teórica correspondente, bastando trabalhar com os polinômios homogêneos. Assim, todas as variedades são K-definíveis em potências de K de uma forma especial.

Por exemplo, se L é um corpo extensão de K ou subcorpo contendo os coeficientes de $f_1, \ldots, f_r, g_1, \ldots, g_s$ (ou outros polinômios equivalentes), definimos $V(L) = Z_L(f_1, \ldots, f_r) - Z_L(g_1, \ldots, g_s)$. Sabemos que, se L também é algebricamente fechado, então a extensão é elementar e $V(L)$ é definido em L pela mesma fórmula (sem quantificadores) com parâmetros em K que define V em K, notadamente

$$\bigwedge_{i=1}^{r}(f_i(v) = 0) \wedge \neg \bigwedge_{j=1}^{s}(g_s(v) = 0)\,.$$

Isso mostra, em particular, que $V(L)$ independe dos polinômios que definem V quando L é algebricamente fechado, porque as fórmulas com parâmetros em K que equivalem em K equivalem em L. Se L é qualquer, podemos considerar seu fecho algébrico tradicional L', que é um corpo algebricamente fechado imerso em ou extensão de K de modo elementar. Então $V(L')$ está bem-definido e as seqüências de elementos de L que satisfazem essas fórmulas são as mesmas, porque as fórmulas não têm quantificadores e $L \subseteq L'$, de modo que $V(L)$ está bem-definido.

Verificaremos agora que, no caso de V ser fechada (afim ou projetiva), então também $V(L)$ é irredutível.

Proposição 6.4.1. Suponha $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ e L corpo algebricamente fechado extensão ou subcorpo de K contendo os coeficientes desses polinômios. Se $F = Z_K(f_1, \ldots, f_r)$ é um fechado irredutível de K^n, também $F(L) = Z_L(f_1, \ldots, f_r)$ é fechado irredutível de L^n.

Demonstração: Vemos que $F(L)$ é fechado por definição, independentemente de F ser irredutível. Suponha F_1, F_2 fechados de L^n contidos propriamente em $F(L)$, tais que $F(L) = F_1 \cup F_2$. Sejam $p_1, \ldots, p_s, q_1, \ldots, q_t \in L[x_1, \ldots, x_n]$ de modo que $F_1 = Z_L(p_1, \ldots, p_s)$ e $F_2 = Z_L(q_1, \ldots, q_t)$.

Considere a sentença σ com constantes em L que afirma (i) $Z(f_1, \ldots, f_r) \subseteq Z(p_1, \ldots, p_s) \cup Z(q_1, \ldots, q_t)$; (ii) $Z(p_1, \ldots, p_s) \subseteq Z(f_1, \ldots, f_r)$; (iii) $Z(q_1, \ldots, q_t) \subseteq Z(f_1, \ldots, f_r)$; (iv) existem raízes comuns de $f_1, \ldots, f_r$ que não são raízes comuns de $p_1, \ldots, p_s$; (v) existem raízes comuns de $f_1, \ldots, f_r$ que não são raízes comuns de $q_1, \ldots, q_t$. A sentença σ traduz, portanto, a situação de $F(L)$, F_1 e F_2, e pode ser escrita explicitamente usando os polinômios, como organizado nos itens (i)–(v). Por exemplo, com v seqüência de n variáveis, (ii) escreve-se

$$\forall v \left(\bigwedge_{i=1}^{s} p_i(v) = 0 \rightarrow \bigwedge_{i=1}^{r} f_i(v) = 0 \right) .$$

Temos $L \models \sigma$. Substitua em σ todas as constantes de L que não pertencem a K por novas variáveis, cuja seqüência indicaremos v, obtendo uma fórmula $\phi(v)$ com parâmetros em K. Note que os polinômios $f_1, \ldots, f_r$ não foram alterados. Temos $L \models \exists v\, \phi(v)$ e, como $(K, (a)_{a \in K}) \equiv (L, (a)_{a \in K})$, também $K \models \exists v\, \phi(v)$. Interpretando conformemente as variáveis de v, obtemos novos polinômios $p_1^*, \ldots, p_s^*, q_1^*, \ldots, q_t^* \in K[x_1, \ldots, x_n]$ que satisfazem as afirmações (i)–(v) substituindo $p_1, \ldots, p_s, q_1, \ldots, q_t$, mas ainda com $f_1, \ldots, f_r$ originais.

Assim, $F = Z(p_1^*, \ldots, p_s^*) \cup Z(q_1^*, \ldots, q_t^*)$ e $Z(p_1^*, \ldots, p_s^*), Z(q_1^*, \ldots, q_t^*)$ estão propriamente contidos em F, contrariando sua irredutibilidade. QED

Corolário 6.4.2. Nessas condições, se V é uma variedade (quase-)afim ou (quase-)projetiva, $V(L)$ também é.

As técnicas que adotaremos a partir de agora só se aplicam a variedades afins, sendo os resultados gerais obtidos considerando-se a cobertura de uma variedade abstrata por afins. Consideraremos, então, essa categoria específica.

Já encontramos no Exemplo 1.3.20 a definição de *ponto genérico* de um espaço topológico: seu unitário é denso no espaço. (Note que o fecho de um unitário é sempre irredutível.) Variedades podem ***não*** conter pontos genéricos: por exemplo, $V = K^1$ é uma variedade afim em que todo conjunto unitário $\{a_1\}$ já é fechado pelo polinômio $x_1 - a_1$. Aliás, em qualquer corpo L extensão de K, $V(L) = L^1$ não contém ponto genérico.

Desse modo, fazemos uma modificação simples, observando que o fato dos parâmetros pertencerem a um conjunto foi recorrente desde o início. Fixados um corpo L extensão de K e V uma variedade afim de K^n, dizemos que $a \in V(L)$ é um *ponto K-genérico* se $a \notin F(L)$ para qualquer fechado F de K^n propriamente contido em V. Note que, neste caso, $F(L)$ é K-definível; se impuséssemos a condição para todo subconjunto fechado próprio de $V(L)$, então realmente a seria um genérico. Por exemplo, um elemento de L transcendente sobre K é um ponto K-genérico de L^1.

Suponha agora L uma extensão elementar de K em que todos os tipos de $S(K)$ sejam realizados. Seja V uma variedade afim de K^n: então $I(V) \in \operatorname{Spec} K[x_1, \ldots, x_n]$ e, pelo mesmo Exemplo 1.3.20, existe um tipo $p \in S_n(K)$ tal que $f \in I(V)$ se e somente se a fórmula $f(v) = 0$ pertence a $p(v)$. Mas $p = t(a/K)$ para algum $a \in L^n$, de modo que $I(V)$ é o conjunto dos polinômios de $K[x_1, \ldots, x_n]$ que se anulam em a. Concluímos que se $F \subset V$ então $I(V) \subset I(F)$ e $a \notin F(L)$, de modo que a é um ponto genérico de $V(L)$. Além dessa existência, vemos que todos os pontos K-genéricos de $V(L)$ têm o mesmo tipo p sobre K, que é exclusivo desses pontos. Novamente, no caso de K^1, é o tipo dos elementos transcendentes.

Já temos as ferramentas necessárias para a identificação central:

Teorema 6.4.3. Se $V \subseteq K^n$ é uma variedade afim, então $\operatorname{RM}(V) = \dim V$.

Demonstração: Procederemos por indução em $\dim V$ como grau de transcendência de $K(V)$ sobre K. Se $\dim V = 0$, sabemos que V é unitário e $\operatorname{RM}(V) = 0$. Suponha então $\dim V = k > 0$ e tome L extensão elementar de K em que todos os tipos de $S(K)$ são realizados. Sabemos que, desse modo, $V(L)$ contém pontos K-genéricos.

Lembre que todos os tipos são da forma $t(a/K)$, $V(L)$ é o definível em L^n correspondente a V e $t(a/K) \in \langle V(L) \rangle \Leftrightarrow V(L) \in t(a/K) \Leftrightarrow a \in V(L)$.

Dado $a \in V(L)$, tome V_a o conjunto dos $x \in K^n$ tais que, para cada $p \in K[x_1, \ldots, x_n]$, se $p(a) = 0$ então $p(x) = 0$. Em outras palavras, $V_a = Z(I_K(a))$ em que $I_K(a)$ é o ideal primo dos polinômios sobre K que se anulam em a. Temos $V_a \subseteq V$ e V_a é uma variedade afim de K^n. Se $V_a \subset V$ propriamente, então $\dim V_a < \dim V$ e $\operatorname{RM}(V_a) \leqslant k - 1$ por indução, donde $\operatorname{RM}(a/K) \leqslant$

$\mathrm{RM}(V_a) \leqslant k-1$. Se $V_a = V$, no caso de a K-genérico, então $I_K(a) = I(V)$ e $K(a) \cong K(V)$ sobre K, e vimos no Exemplo 3.4.7 que $\mathrm{RM}(a/K)$ é o grau de transcendência de $K(a)$ ou $K(V)$ sobre V, ou seja, $\mathrm{RM}(a/K) = k$.

Assim, invocamos a equação de posto $\mathrm{RM}(V) = \max_{a\in V(L)} \mathrm{RM}(a/K) = k$, em que usamos a existência dos pontos K-genéricos para atingir o máximo.

QED

Observamos, porém, que esse resultado pode ser estendido para uma variedade quase-afim U, com fecho V. De fato, $V - U$ é um subconjunto fechado próprio de V e tem dimensão $< \dim V$, donde $\mathrm{RM}(V-U) < \mathrm{RM}(V)$ e $\mathrm{RM}(U) = \mathrm{RM}(V)$. A Proposição I.1.10 de [Hartshorne], por outro lado, calcula $\dim U = \dim V$.

Corolário 6.4.4. Da demonstração, percebemos que $a \in V(L)$ é K-genérico se e somente se $\mathrm{RM}(a/K) = \mathrm{RM}(V)$. Portanto, o único tipo $p \in \langle V\rangle \subseteq S_n(K)$ com posto $\mathrm{RM}(V)$, chamado *genérico*, é o tipo dos pontos K-genéricos. Conclui-se que $\mathrm{dM}(V) = \mathrm{dM}(p) = 1$, porque p é global e $Th(K)$ é totalmente transcendental (K é algebricamente fechado). Em particular, toda curva afim tem posto e grau 1, sendo um conjunto fortemente minimal.

Vimos que, para variedades e morfismos, a locução "definido sobre L" implica a modelo-teórica "L-definível". Reciprocamente, um polinômio com coeficientes em K pode induzir conjunto ou função L-definível, mas isso não significa imediatamente que corresponda a um polinômio com coeficientes em L. Trabalharemos sobre essa questão, agora, lembrando que K é algebricamente fechado.

Lema 6.4.5. Seja $F \subseteq K^n$ um fechado de Zariski. Então F tem um menor corpo de definição $K_0 \subseteq K$. Todo automorfismo de K fixa F se e somente se fixa os elementos de K_0.

Referência: O Fato 2.6 de [Pillay A].

Corolário 6.4.6. Sejam $F \subseteq K^n$ um fechado de Zariski e L um subcorpo de K. Então F é L-definível (modelo-teoricamente) se e somente se F está definido sobre o fecho perfeito de L, que sabemos ser $\mathrm{dcl}(L)$.

Demonstração: Seja K_0 o menor corpo de definição, dado pelo lema. Se F é L-definível, então todo automorfismo de K sobre L fixa F e, pelo lema, fixa os elementos de K_0. Desse modo, $K_0 \subseteq \mathrm{DCL}(L) = \mathrm{dcl}(L)$.

Reciprocamente, se F está definido por polinômios com coeficientes em $\mathrm{dcl}(L)$, então cada um desses coeficientes é definido por uma fórmula com parâmetros em L, de modo que F é L-definível. QED

Corolário 6.4.7. Se L é um subcorpo perfeito de K, caso dos corpos algebricamente fechados, então as locuções "definido sobre L" e "L-definível" equivalem para variedades afins.

Considere agora um grupo algébrico G, cuja variedade é afim: $\mathrm{dM}(G) = 1$ e então $G = G^0$. O caso geral é discutido pelo Lema 4.4 de [Pillay A] e a pág. 28 de [Hindry, Silverman]: quando a definição de grupo algébrico é relaxada a conjuntos redutíveis, suas componentes irredutíveis são duas a duas disjuntas, portanto conexas; a componente que contém o elemento neutro é única e indicada G^0 — daí o nome "componente conexa", e G^0 é uma definição de Chevalley.

Lema 6.4.8. Um subgrupo definível de um grupo algébrico é fechado, portanto subgrupo algébrico.

Demonstração: Sejam H um subgrupo definível de um grupo algébrico G e H_1 seu fecho, que já sabemos ser um subgrupo de G. Mas H é união finita de conjuntos da forma $Y - Z$ em que Y é fechado irredutível, contido em H_1, e Z um subconjunto fechado próprio de Y. Seja U a união desses conjuntos quando $\mathrm{RM}(Y)$ é máximo. Então $\mathrm{RM}(H_1 - U) < \mathrm{RM}(H_1)$ e $U \subseteq H$. Assim, todo tipo genérico de H_1 contém H. Como vimos no Capítulo 5, $HH = H_1$ e $H = H_1$. QED

Lema 6.4.9. Sejam G, H grupos algébricos e $f : G \to H$ um homomorfismo definível. Se K tem característica 0 então f é um morfismo; se K tem característica $p > 0$ então f é um p-morfismo, isto é, composta de morfismo com potências da função $(\cdot)^{-p}$.

Referência: O Lema 4.9 de [Pillay A].

Proposição 6.4.10. Seja G um grupo definível em K. Então G é definivelmente isomorfa a um grupo algébrico. Ao menos quando K tem característica 0, se K_0 é um subcorpo de K sobre o qual G é definível, então o isomorfismo e o grupo algébrico podem ser considerados definidos sobre K_0.

Referência: A Proposição 4.12 de [Pillay A].

Proposição 6.4.11. Seja F um corpo infinito definível em K. Então F é definivelmente isomorfo a K.

Referência: A Proposição 4.13 de [Pillay A].

A Observação 2.14(ii) de [Pillay A] sugere que se incorporem os pontos de vista de folheações e esquemas na abordagem modelo-teórica.

O leitor que deseja conhecer imediatamente a Conjectura de Mordell–Lang e seu enunciado modelo-teórico pode, agora, avançar diretamente para o último capítulo.

7
Geometrias de Zariski

Este capítulo sintetiza o artigo [Hrushovski, Zilber] e as adaptações necessárias de [Hrushovski], acompanhado de informações de [Marker A], preparando-nos para o desfecho da Conjectura de Mordell–Lang. Trata-se do último trabalho de Hrushovski na seqüência de estudos que o levou à percepção modelo-teórica da Geometria Algébrica, antes da prova da conjectura. O estudo completo de [Hrushovski, Zilber] merece uma dissertação específica, que se baseie também nesses outros artigos, retroativamente. Suas longas passagens técnicas, sem omitir demonstrações ou referências aos textos anteriores de Hrushovski, justificam duplamente esta abordagem.

Desse modo, contentamo-nos em expor seu conteúdo, ajustando alguns pré-requesitos aos tópicos que já desenvolvemos para usufruir de seus resultados, e indicando alguns pontos que nos pareceram mais importantes para que o leitor interessado consulte-o diretamente. Não definiremos, contudo, todos os termos que lá são definidos.

O artigo homônimo dos dois autores em 1993 (Bulletin AMS, vol. 28, no. 2, p. 315–323) contém uma aplicação às variedades complexas e roteiros globais das demonstrações.

Este capítulo não é necessário para a apresentação da Conjectura de Mordell–Lang e seu enunciado modelo-teórico.

Para $Z \subseteq X \times Y$ e $x \in X$, escreva $Z_x = \{y \in Y \mid (x, y) \in Z\}$ — em [Hrushovski, Zilber] e [Marker A], indica-se $Z(x)$. Nesse contexto, como usual, lemos $D^n \times D^m = D^{n+m}$ e a topologia não é produto, mas aquela dada pela definição.

As geometrias de Zariski são uma classe importante para a qual é verdadeira a Conjectura de Zilber. De fato, reescreveremos os resultados da Seção 4.4 e veremos que uma geometria de Zariski não é localmente modular se e somente se é ampla. Após o Teorema 7.1.7, concluiremos que uma geometria de Zariski ampla interpreta um corpo algebricamente fechado.

7.1. Definições e os teoremas principais

Trabalharemos novamente com espaços noetherianos de dimensão finita.

Apresentaremos imediatamente a definição de geometrias de Zariski, seguindo-a das motivações dos itens (Zn) e do exemplo fundamental.

Definição 7.1.1. Uma *geometria de Zariski* é um conjunto infinito D, acompanhado de uma topologia noetheriana em cada D^n, $n \in \mathbb{N}^*$, satisfazendo estas condições:

(Z0) (i) Sejam $f_i : D^n \to D$, $1 \leqslant i \leqslant k$, funções cada uma constante ou projeção (da forma $f_i(x_1, \ldots, x_n) = x_{j_i}$). Seja $f : D^n \to D^k$ definida por $f(x) = (f_1(x), \ldots, f_k(x))$. Então f é contínua. (ii) As diagonais $\Delta_{i,j} = \{x \in D^n \mid x_i = x_j\}$ são fechadas.

(Z1) Sejam $Y \subseteq D^n$ fechado irredutível e $\pi : D^n \to D^k$, $\pi(x_1, \ldots, x_n) = (x_{i_1}, \ldots, x_{i_k})$, uma projeção. Então existe um subconjunto fechado próprio F de $\mathrm{cl}(\pi[Y])$ tal que $\mathrm{cl}(\pi[Y]) - F \subseteq \pi[Y]$.

(Z2) (i) D é irredutível. (ii) Se $Y \subseteq D^k \times D$ é fechado, existe $m \in \mathbb{N}^*$ tal que, para cada $a \in D^k$, $Y_a = D$ ou $|Y_a| \leqslant m$. Em particular, com $k = 0$, todo subconjunto fechado próprio de D é finito.

(Z3) $\dim(D^n) \leqslant n$. Se Y é um fechado irredutível de D^n, então toda componente de $Y \cap \Delta_{i,j}$ tem dimensão $\geqslant \dim Y - 1$.

Um *isomorfismo* entre geometrias de Zariski D, E é uma bijeção entre D e E que induz um homeomorfismo entre D^n e E^n, para cada $n \in \mathbb{N}^*$.

Os comentários de [Hrushovski, Zilber] sobre essas condições são essenciais:

(Z0) generaliza a condição de D^n ter a topologia produto e relaciona as diversas topologias presentes. Por exemplo, suponha $F \subseteq D^n \times D^m$ fechado e $a \in D^n$: então F_a é fechado, porque a função $f : D^m \to D^{n+m}$, $f(x) = (a, x)$, é contínua por (Z0) e $F_a = f^{-1}[F]$. Em particular, podemos tomar $n = m$ e $F = \Delta_{1,n+1} \cap \Delta_{2,n+2} \cap \ldots \cap \Delta_{n,n+n}$ fechado também por (Z0), caso em que $F_a = \{a\}$ e concluímos que os conjuntos unitários de n-uplas são fechados (irredutíveis então).

(Z1) também é uma generalização: da condição de D ser *completa*, isto é, todas as projeções serem fechadas. Sua formulação, porém, não exclui curvas afins. Veremos que se trata de uma forma de eliminação de quantificadores.

Já observamos na definição a conseqüência de (Z2) de que todo fechado próprio de D é finito.

(Z3) dá uma teoria de dimensão, chave para todo o artigo em seus lemas técnicos. Embora já possa ser chamada de "Teorema de dimensão", reserva-se esse título para sua generalização no Teorema 7.2.4. Prioritariamente, (Z3) informa que as dimensões dos D^n são finitas.

Mostra-se que $\dim(X \times Y) = \dim X + \dim Y$; por (Z2) obtemos $\dim D = 1$, donde $\dim(D^n) = n$.

Exemplo 7.1.2. Seja C uma curva quase-projetiva suave sobre um corpo algebricamente fechado, com C^n com a topologia induzida pela topologia de Zariski. Argumentaremos que C torna-se uma geometria de Zariski.

Como a topologia de Zariski é noetheriana, também a topologia de cada C^n é noetheriana.

A condição (Z0) é verificada porque trata, de fato, de funções com componentes polinomiais e conjuntos de raízes de polinômios.

Considere agora a condição (Z1), com a notação da definição. Por eliminação de quantificadores no corpo algebricamente fechado, existem fechados irredutíveis $F_1, \ldots, F_m \subseteq C^k$ e fechados $E_i \subseteq F_i$ com $\pi[Y] = \bigcup_{i=1}^m (F_i - E_i)$. Então $\mathrm{cl}(\pi[Y]) = \bigcup_{i=1}^m F_i$ e $\bigcup_{i=1}^m F_i - \bigcup_{i=1}^m E_i \subseteq \pi[Y]$.

Quanto a (Z2), note que C é irredutível na topologia de Zariski e portanto em si mesma. Já que tem posto e grau de Morley (dimensão e irredutibilidade de variedade, respectivamente) iguais a 1, é fortemente minimal, de modo que a Proposição 1.3.7 implica que, para qualquer definível $Y \subseteq C^k \times C$ existe $m \in \mathbb{N}^*$ tal que, para qualquer $a \in C^k$ $|Y_a| \leqslant m$ ou $|C - Y_a| \leqslant m$. Se Y é fechado, então Y_a é fechado; neste caso, se Y_a também for infinito, então $Y_a = C$.

Para a condição (Z3), a propriedade de suavidade torna-se importante, porque então cada C^n será uma variedade suave. Referimos o leitor ao apêndice de [Marker A]. Essa referência apresenta, contudo, a curva $y^2z = x^3 + x^2z$ em $\mathbb{P}^2$ sem (Z3) e a curva $y^2z = x^3$ em $\mathbb{P}^2$ com singularidade e (Z3).

Definição 7.1.3. Suponha D geometria de Zariski.

(i) Uma *curva plana* é um subconjunto irredutível de D^2 com dimensão 1. Uma *família de curvas planas*, parametrizada por um fechado irredutível $X \subseteq D^n$, é um fechado irredutível $C \subseteq X \times D^2$ de modo que C_x é uma curva plana para cada $x \in X$ genérico.

(ii) Diz-se que D é *ampla* se existe uma família de curvas planas $C \subseteq X \times D^2$ como acima de modo que, para cada dois pontos genéricos $p, q \in D^2$ distintos, existe uma curva C_x contendo p e q. Diz-se ainda que D é *muito ampla* se também, para quaisquer $p, q \in D^2$, existe C_x contendo apenas um de p, q.

[Marker A], em um exemplo na pág. 115, afirma que a geometria de Zariski de uma curva suave é muito ampla.

Enunciamos agora os teoremas apresentados por [Hrushovski, Zilber] em sua introdução. Comentaremos sobre a localização das demonstrações em nossa Seção 7.5. Este resultado constitui-se do Teorema A de [Hrushovski, Zilber]:

Teorema 7.1.4 (A). Seja D uma geometria de Zariski muito ampla. Então existe uma curva quase-projetiva suave C sobre um corpo algebricamente fechado K tal que D e C são isomorfas como geometrias de Zariski. A curva C

é completa se e somente se a geometria D é completa, isto é, se todas as suas projeções são fechadas.

A curva C é essencialmente única, como mostra sua Proposição 1.1:

Proposição 7.1.5 (1.1). Sejam C, C' curvas suaves sobre corpos algebricamente fechados K, K' respectivamente e $h : C \to C'$ um isomorfismo de geometrias de Zariski. Então há um isomorfismo de corpos $h_0 : K \to K'$ e, identificando-se K e K' por h_0, a função h torna-se um isomorfismo de variedades algébricas.

Definição 7.1.6. Suponha D, E geometrias de Zariski. Uma função $f : D \to E$ é dita *de Zariski* se induz uma função contínua em cada D^n. Diz-se que f é *fechada* se ainda a função induzida em cada D^n é fechada, ou seja, leva fechados a fechados.

Dada a ambigüidade com funções fechadas (usuais), escreveremos "função de tipo **Z**" e "função de tipo **ZF**" para denotar, respectivamente, funções de Zariski comuns e fechadas.

Com essa definição, enuncia-se seu Teorema B:

Teorema 7.1.7 (B). Se D é uma geometria de Zariski ampla, existem um corpo algebricamente fechado K e uma função de tipo **Z** sobrejetora $f : D \to \mathbb{P}^1(K)$. A imagem de um construtível por f é (algebricamente) construtível. Para algum $F \subseteq D$, finito, f é de tipo **ZF** em $D - F$.

Como observado na página 6 do artigo, tal função f tem fibras finitas, isto é, a imagem inversa $E_f = f^{-1}[\{x\}]$ é finita para cada $x \in \mathbb{P}^1$. Desse modo, $\mathbb{P}^1$ é interpretado em D, mais precisamente isomorfo a D/E_f, porque E_f é uma relação de equivalência fechada. Além disso, nenhuma estrutura extra é induzida em $\mathbb{P}^1$ a partir de D; todo automorfismo de $\mathbb{P}^1$ estende-se a automorfismo de D. Desse modo, D pode ser visto como uma cobertura finita de $\mathbb{P}^1$. Conclui-se que D interpreta K. Daremos significado preciso às interpretações, porque precisamos definir a linguagem apropriada, na próxima seção.

Finalmente,

Teorema 7.1.8 (C). Existe uma geometria de Zariski D completa, ampla e unidimensional que não pode ser interpretada em um corpo algebricamente fechado. Em particular, se C é uma curva sobre um tal corpo, toda função $f : C \to D$ de tipo **Z** é constante.

7.2. A linguagem de uma geometria

Vimos na Seção 1.3 que uma estrutura da Teoria dos Modelos pode ser descrita sem prévia definição de linguagens, mas tomando-se a família de seus $\emptyset$-definíveis como informação primitiva. De um modo análogo, obteremos uma linguagem de primeira ordem para uma geometria de Zariski fixada.

Seja então D uma geometria de Zariski. Defina a linguagem L_D tomando um predicado n-ário para cada subconjunto fechado de D^n. A interpretação natural desse predicado é o próprio fechado, e obtemos uma L_D-estrutura $\mathfrak{D}$ com domínio D.

Assim, todo fechado é definível e, então, todo construtível é definível. Veremos que há eliminação de quantificadores e obteremos a recíproca.

Note que os automorfismos de D, como geometria de Zariski, são permutações de D que induzem homeomorfismos; em particular, levam fechados a fechados. Por outro lado, os automorfismos modelo-teóricos de $\mathfrak{D}$ são as bijeções que fixam esses fechados e são, portanto, automorfismos de D.

Define-se também a linguagem $\mathrm{L}_{\mathrm{nat}D}$ redução de L_D que contém somente os predicados dos fechados invariantes sob os automorfismos da geometria D. Esta é a chamada *linguagem natural* de D.

Atenção: modificamos, por razões de compatibilidade, as notações originais $L(D)$ e $L_{\mathrm{nat}}(D)$ de [Hrushovski, Zilber].

No Teorema B, K e f podem ser escolhidos $\emptyset$-definíveis em $\mathrm{L}_{\mathrm{nat}D}$, obtendo-se o Teorema B′:

Teorema 7.2.1 (B′). Se D é uma geometria de Zariski ampla, existem um corpo algebricamente fechado K, uma curva C suave sobre K e uma função $f : D \to C$ de tipo $\mathbf{Z}$ sobrejetora de fibras finitas, todos $\emptyset$-definíveis em $\mathrm{L}_{\mathrm{nat}D}$.

A Proposição 2.1 de [Hrushovski, Zilber], demonstrada em sua pág. 8, generaliza o Teorema de Tarski–Chevalley:

Teorema 7.2.2. Em uma geometria de Zariski, a projeção de um conjunto construtível é construtível. Toda estrutura associada a uma geometria de Zariski admite, portanto, eliminação de quantificadores, e todo conjunto definível é construtível.

Neste contexto, uma fórmula da forma $\exists v\, \phi$, com ϕ sem quantificadores, corresponde à projeção usual de uma combinação booleana finita de fechados, aqueles cujos predicados (de L_D) ocorrem em ϕ.

Corolário 7.2.3. A estrutura $\mathfrak{D}$ de uma geometria de Zariski D é fortemente minimal.

Demonstração: Este é o Corolário 2.7 de [Hrushovski, Zilber]. Seja $E \subseteq D^n \times D$ um definível, portanto construtível. Tome $E = X - F$ com X, F fechados. Para $a \in D^n$, se X_a é finito, então E_a é finito, com a mesma limitação. Então basta aplicar (Z2) a X e F, pela Proposição 1.3.7. QED

Para provar sua Proposição 2.1, o artigo demonstra alguns lemas técnicos de interesse próprio, como por exemplo o fato de D^n ser irredutível para todo $n \in \mathbb{N}^*$ (Lema 2.2). Remetemos o leitor ao próprio artigo, mas destacamos o Lema 2.5 que generaliza a condição (Z3):

Teorema 7.2.4 (Dimensão). Sejam $F_1, F_2 \subseteq D^n$ fechados irredutíveis que se intersectem e W uma componente irredutível qualquer de $F_1 \cap F_2$. Então $\dim W \geqslant \dim F_1 + \dim F_2 - n$.

Observamos que

Teorema 7.2.5. Uma geometria de Zariski não é localmente modular se e somente se é ampla.

Referência: O Lema 3.1 de [Marker A].

Façamos agora um breve salto, para a Seção 4 do artigo.

Suponha $\mathfrak{A}$ uma L_D-estrutura. Definiremos os conjuntos fechados em A^n. Dados $F \subseteq D^m \times D^n$ fechado com predicado $(m+n)$-ário P e $a \in A^m$, lembramos que P tem uma interpretação $P(\mathfrak{A})$ em E^{m+n}. Então definimos que o conjunto $P(\mathfrak{A})_a$ é um fechado; na notação de definíveis, trata-se do conjunto $P(a, (\mathfrak{A}) \subseteq A^n$. Chamamos 0-fechado quando $m = 0$, por analogia com os $\emptyset$-definíveis.

Suponha $\mathfrak{D} \prec \mathfrak{D}'$, e que o domínio desta estrutura seja $E = D'$. Podemos aplicar essa construção a $\mathfrak{D}'$, de modo que

Teorema 7.2.6. Obtivemos realmente uma topologia noetheriana em cada E^n, com as quais E é uma geometria de Zariski. Sua linguagem apropriada L_E expande L_D e o reduto de $\mathfrak{E}$ a L_D é a estrutura $\mathfrak{D}'$, obtida com os casos $m = 0$. Caso D seja completa, também E é completa.

Referência: A Proposição 4.1 de [Hrushovski, Zilber], provada nas páginas 14 e 15 do artigo, que também apresenta uma versão curta da demonstração devida a Ziegler.

Desse modo, podemos seguir o padrão modelo-teórico: o artigo convencionará trabalhar com um modelo monstro, como veremos na próxima seção. Como em [Marker A] — que indica $D_0 \prec D$ — podemos, a partir de D, considerar o modelo monstro extensão $\mathfrak{D}'$ e a geometria da estrutura $\mathfrak{C}$. Cuidado: neste momento, $\mathfrak{D}$ e $\mathfrak{C}$ não são estruturas com a mesma linguagem apropriada.

O restante da Seção 4 é técnico; optamos por destacar somente a

Definição 7.2.7. Suponha $\mathfrak{A}, \mathfrak{B} \models Th(\mathfrak{D})$. Uma *especialização* é um homomorfismo na linguagem L_D entre $X \subseteq A$ e B, isto é, uma função $h : X \to B$ tal que, se $x \in X^n$ pertence à interpretação em $\mathfrak{A}$ de um predicado P de L_D, então $h(x)$ pertence à interpretação de P em $\mathfrak{B}$. Note que essas interpretações correspondem precisamente aos conjuntos 0-fechados.

Trata-se de uma linguagem (em termos matemáticos de "ferramenta") equivalente àquela de conjuntos fechados: veremo-la em ação para definir tangência na Seção 7.4. A Proposição 4.4 do artigo mostra que, na notação acima e no caso de uma geometria completa, toda especialização estende-se a todo A.

Pré-requesitos em Teoria dos Modelos

A terceira seção de [Hrushovski, Zilber] sumariza os conhecimentos necessários de Teoria dos Modelos para sua leitura. Dedicamo-nos, agora, a estabelecer a equivalência de sua formulação com a que já estudamos, para usufruir de seus resultados. Observamos que, como em outros artigos desta área, sua formulação é a mais breve possível e baseada em definíveis. É o caso da definição de estruturas por $\emptyset$-definíveis.

Quanto a um modelo monstro, associa a cada estrutura $\mathfrak{A}$ uma extensão elementar $\mathfrak{A}^*$, ω_1-compacta e fortemente ω_1-homogênea, que assume existir. De fato, o artigo trabalha em $\mathfrak{A}^*$ e não em $\mathfrak{A}$, ou melhor, em $(\mathfrak{A}^*)^{\mathrm{eq}}$ finalmente. (Observamos que as letras usadas são M, N, M^*, como na literatura moderna.)

Na Seção 2, o artigo já havia definido estruturas fortemente minimais por meio de nossa Proposição 1.3.7.

Também vimos sua formulação de interpretação na Proposição 4.1.2. Sua construção da estrutura $\mathfrak{A}^{\mathrm{eq}}$ é semelhante à que apresentamos, mas com fórmulas que definem relação de equivalência sobre um subconjunto definível em vez de todo o domínio: veja na demonstração da Proposição 4.3.2 como abordamos esse caso.

Seus fechos definível e algébrico são idênticos aos nossos.

Sua definição de posto de Morley equivale, como vimos estudando o grau, à que apresentamos para posto interno e equivale no nosso modelo monstro ω-saturado. Desse modo, a correspondência estende-se ao posto de tipos. O artigo escreve rk e indica $\mathrm{rk}(\emptyset) = -\infty$. O posto de um definível é a dimensão de seu fecho.

O artigo define que $a_1, \ldots, a_n$ são *independentes* sobre X se $\text{rk}(a_1, \ldots, a_n/X) = \sum_{i=1}^{n} \text{rk}(a_i/X)$, o que equivale com independência sobre $\text{acl}(X)$, como estudamos.

Uma nota da pág. 112 de [Marker A] apresenta este lema como conseqüência das relações de posto:

Lema 7.2.8 (Fibras genéricas). Sejam $X \subseteq D^{m+n}$ e $\pi : D^m \times D^n \to D^n$ a projeção usual. Se $a \in \text{cl}(\pi[X])$ é genérico, então $\dim X = \dim \text{cl}(\pi[X]) + \dim \pi^{-1}[\{a\}]$.

7.3. "Eliminação de imaginários"

Trabalharemos sobre a homônima Seção 5 de [Hrushovski, Zilber]. Novamente em sua pág. 112, [Marker A] argumenta que, em geral, geometrias de Zariski não têm eliminação de imaginários.

Definição 7.3.1. Suponha $n \in \mathbb{N}^*$ e H subgrupo do grupo $S_n = \text{Sym}(n)$ das permutações de n elementos, que age sobre D^n permutando coordenadas. O espaço $S_H = D^n/H$ das órbitas sob H é chamado *tipo especial* (em inglês, *special sort*).

Seja $\pi : D^n \to S$ a projeção natural. Topologizamos S assim: $F \subseteq S$ é fechado se $\pi^{-1}[F]$ é fechado.

Definição 7.3.2. Definiremos regularidade para pontos de vários conjuntos: suponha $p \in F$.

(i) $F \subseteq D^n$ fechado irredutível. Seja $\Delta_F = \{(x, y) \in F \times F \mid x = y\}$. p é um *ponto regular* de F se existe um fechado irredutível $Y \subseteq D^n \times D^n$ tal que $\dim(D^n \times D^n) - \dim Y = \dim F$ e Δ_F é a única componente de $Y \cap (F \times F)$ contendo (p, p).

(ii) $F \subseteq D^n$ fechado qualquer. p é um *ponto regular* de F se está contido em uma única componente de F, cuja dimensão seja $\dim F$, e é ponto regular dessa componente.

(iii) Com a notação de definição anterior, F fechado de S. p é um *ponto regular* de F se é imagem por π de um ponto regular de $\pi^{-1}[F]$.

$U \subseteq S$ é *regular* se U é aberto de $\text{cl}(U)$ e todo ponto de U é regular em $\text{cl}(U)$. Vemos que S é regular.

O leitor pode agora, por ter as definições necessárias, saltar diretamente para a definição de atlas. Optamos, entretanto, por elencar alguns resultados importantes.

Lema 7.3.3 (Lascar–Pillay). Suponha D um conjunto fortemente minimal e $\mathrm{acl}(\emptyset) \cap D$ infinito. Para cada tipo imaginário S existe uma partição de S em um número finito de $\emptyset$-definíveis X_i, tipos especiais S_i e funções $\emptyset$-definíveis injetoras $f_i : X_i \to S_i$. Equivalentemente, para todo elemento imaginário e existe e' de um tipo especial tal que $\mathrm{dcl}(e) = \mathrm{dcl}(e')$.

Referência: O Lema 5.1 de [Hrushovski, Zilber].

O Teorema de Dimensão estende-se aos tipos especiais, como mostra o Lema 5.2 de [Hrushovski, Zilber].

O Lema 5.3 de [Hrushovski, Zilber] mostra que, se F é um fechado de S, então os pontos regulares de F formam um subconjunto aberto denso. O Lema 5.4 de [Hrushovski, Zilber] generaliza novamente o Teorema de Dimensão.

[Marker A] indica, nas p. 113–114, que em uma variedade algébrica todo ponto não-singular é regular.

Definição 7.3.4. Um *atlas* é um conjunto M, acompanhado de um número finito n de injeções $f_i : U_i \to M$ em que cada U_i é subconjunto regular irredutível de um tipo especial, $\bigcup_{i=1}^{n} f_i[U_i] = M$ e cada $\{(x,y) \in U_i \times U_j \mid f_i(x) = f_j(y)\}$ é subconjunto irredutível de $U_i \times U_j$ projetando sobre um aberto não-vazio de U_i. (Evitamos a tradução *variedade* do termo inglês *manifold*, porque já a usamos para *variety* e ambos os conceitos ocorrem neste capítulo.)

Suponha M, N atlas com $f_i[U_i]$ cobrindo M e $g_j[V_j]$ cobrindo N.

Para abertos de uma topologia sobre M, tomamos os conjuntos $A \subseteq M$ tais que $f_i^{-1}[A]$ é aberto em U_i para cada i. Desse modo, a terceira condição da definição e o Lema 5.5 de [Hrushovski, Zilber] implicam que cada f_i é um homeomorfismo entre U_i e $f_i[U_i]$. M torna-se noetheriano irredutível, com a mesma dimensão que qualquer U_i, e o Teorema de Dimensão vale em M.

Naturalmente, $f_i[U_i] \times g_j[V_j]$ cobrem $M \times N$ e dão ao produto uma estrutura de atlas, incluindo topologia.

Definição 7.3.5. $\alpha : M \to N$ é um *morfismo* se seu gráfico é um fechado irredutível de $M \times N$. Não confundir com homomorfismo de geometrias de Zariski induzidas, aos quais [Hrushovski, Zilber] refere-se como especializações.

Lema 7.3.6. Dada uma função $\alpha : M \to N$, equivalem: α é um morfismo; para todo j, $\alpha^{-1}[V_j]$ é aberto em M e $\alpha|_{\alpha^{-1}[V_j]}$ é um morfismo; para todo i, $\alpha|_{U_i}$ é um morfismo. Todo morfismo é contínuo e a composição de morfismos é morfismo. Dados morfismos $\alpha_k : M_k \to N_k$, $k \in \{1,2\}$, o natural $\alpha : M_1 \times M_2 \to N_1 \times N_2$, $\alpha(x,y) = (\alpha_1(x), \alpha_2(y))$, é morfismo.

Referência: Os lemas numerados de 5.7 a 5.10 em [Hrushovski, Zilber].

Lema 7.3.7. Se G é um grupo definível em uma geometria de Zariski D, então G pode ser dotado de uma estrutura de atlas, de modo que seu produto $G^2 \to G$ e sua inversão $G \to G$ são morfismos. Essa estrutura de atlas é única, a menos de isomorfismo de atlas. Se G é conexo, ou seja, sem subgrupo definível próprio de índice finito, então o atlas é irredutível.

Referência: O Lema 5.11 e a Observação 5.12 de [Hrushovski, Zilber].

O restante da seção, na página 25, é técnico e trabalha sobre os tecnicismos que omitimos da Seção 4.

7.4. "Interpretando o corpo"

Traduziremos livremente, da seção homônima de [Hrushovski, Zilber], a introdução 6.1.

Para interpretar um corpo F na geometria de Zariski D, o artigo trabalhará na categoria dos conjuntos e funções definíveis, em vez da categoria mais fina de fechados. A estrutura de Zariski surgirá apenas através da noção de especialização. Esta é uma descrição da demonstração em termos gerais.

Suponha primeiramente que D é de fato a reta afim $\mathbb{A}^1(K)$ sobre um corpo algebricamente fechado K. Seja F uma família de curvas em D^2, todas passando pelo ponto $p = (0, 0)$. Assuma que cada curva C em F é o gráfico de uma função suave em p. Então podemos ver $C_i \in F$ codificando a inclinação σ_i de C_i em p. A composição

$$C_1 \circ C_2^{-1} = \{(x, y) \in D^2 \mid \text{existe } z \in D \text{ tal que } (z, x) \in C_2 \text{ e } (z, y) \in C_1\}$$

tem inclinação σ_1/σ_2. Portanto, neste caso interpretaremos uma cópia do grupo multiplicativo se definirmos a relação de tangência de duas curvas em p. Podemos fazê-lo assim: as curvas C_1 e C_2 são *tangentes* em p se existem curvas genéricas $C_1^*, C_2^* \in F$ intersectando-se em dois pontos distintos q, q' e existe uma especialização levando C_i^* a C_i e mapeando ambos q, q' a p.

Essa idéia pode realmente ser desenvolvida, mesmo que as curvas C_i não sejam gráficos de funções racionais. Porém, o grupo obtido desse modo nem sempre é o grupo multiplicativo, porque todas as curvas podem ter mesma inclinação em p e neste caso o processo distingüirá a segunda derivada (ou de ordem maior). Não nos preocuparemos com a natureza do grupo, e escreveremo-lo aditivamente $(A, +, 0)$. (A operação de grupo será diferenciada novamente, e o resultado será o grupo aditivo de qualquer modo.)

Agora, suponha que D é uma curva sobre um corpo algebricamente fechado K, mas não necessariamente racional. Então existe uma correspondência finito-a-finito α entre D e K. Encontramos uma família F de curvas sobre D^2, todas passando através de um ponto $p_0 \in D^2$. Através de α, F origina uma família F' de curvas sobre $K^2 = (\mathbb{A}^1(K))^2$, passando através do ponto q_0; C corresponde a qualquer componente C' da curva $\alpha \circ C \circ \alpha^{-1}$. Esta correspondência também é finito-a-finito. Assim, devemos reconhecer um grupo tranformado por uma correspondência finito-a-finito: a Subseção 6.2 do artigo ocupa-se disso.

Uma vez que temos um grupo abeliano H, podemos repetir o processo com mais informações à nossa disposição. Dada uma família de funções de H a H, podemos somá-las ponto a ponto e compô-las. As duas operações, vistas agindo sobre o espaço tangente, simultaneamente produzem uma estrutura de corpo.

Algumas dificuldades técnicas surgem quando esse plano é desenvolvido. Em geral, não é claro por que a noção de tangência definida acima não será degenerada (por exemplo, $C_1 \circ C_2^{-1}$ é tangente a $C_3 \circ C_4^{-1}$ se e somente se duas das quatro curvas são iguais). Mostraremos que este não é o caso explorando certas simetrias da situação e mostrando que de fato qualquer degenerescência introduziria uma assimetria. Contudo, a necessidade de registrar essas simetrias leva a uma apresentação mais técnica que o esboço acima sugere.

O artigo assume então D fortemente minimal. Na Subseção 6.2, pode-se supô-la apenas minimal em alguma estrutura saturada, em que $\mathrm{dcl}(\emptyset) = \mathrm{acl}(\emptyset)$ é infinito. Em 6.3, pode-se supô-la apenas infinitamente definível, isto é, intersecção de uma família infinita de definíveis, e minimal em alguma estrutura saturada.

Proposição 7.4.1. (i) Se D não é degenerada, isto é, contém outras famílias não-constantes de curvas planas além de $\{a\} \times D$ e $D \times \{a\}$, então existe um grupo abeliano, definível em D, unidimensional.

(ii) Se D é ampla (não é localmente modular), então D interpreta um corpo unidimensional.

Referências: Os Lemas 6.10 e 6.11 de [Hrushovski, Zilber].

7.5. Conclusão do artigo

A sétima seção de [Hrushovski, Zilber] mostra, em especial a Proposição 7.10 provada na página 41, que as topologias de Zariski e a induzida no atlas pela geometria de Zariski coincidem no corpo encontrado na seção anterior. Diz-se que o corpo é *puro*.

A Seção 8 prova o Teorema B (impresso no local como D) e a Proposição 1.1 do artigo. Para o primeiro, usa-se o Teorema de Macintyre, mas há um argumento que o evita.

Estes são os dois fatos lembrados na Observação 8.1: (i) Do ponto de vista modelo-teórico, K é interpretável em D e a estrutura induzida é o corpo puro, com um subcorpo de elementos distinguidos; (ii) Pode-se mostrar para conjuntos fortemente minimais D, em geral, que se (i) vale então K pode ser interpretado sem parâmetros.

Embutidos na demonstração do Teorema B, estão os Lemas 8.2 e 8.3, que enunciam respectivamente: existe um morfismo não-constante de D a $\mathbb{P}^1$ e todo morfismo sobrejetor de D a $\mathbb{P}^1$ é uma função de Zariski fechada em algum subconjunto cofinito de D.

Não faremos, sobre a Seção 9 de [Hrushovski, Zilber], mais do que observar que demonstra os Teoremas A e B′, após resultados técnicos, e apresenta dois exemplos. O Exemplo 9.10 mostra que nem todo subconjunto fechado de D^n é definível em $\mathrm{L}_{\mathrm{nat}D}$ com parâmetros em D. O Exemplo 9.11 mostra que, na linguagem natural de um atlas de dimensão > 1, não mais se pode achar um corpo $\emptyset$-definível.

A Seção 10 considera grupos abstratos G agindo sobre geometrias de Zariski X de modo que cada $g \in G$ torna-se um morfismo. A ação é chamada *semi-livre* se cada órbita de G sobre X é regular ou degenerada, assim: se $gx = x$ então $g = 1$ ou, para todo $g' \in G$, $g'x = x$.

Proposição 7.5.1. Nessa situação, seja $i : G^* \to G$ um homomorfismo de grupos com núcleo finito H. Então existem geometria de Zariski X^*, ação semi-livre de G^* sobre X^* e $j : X^* \to X$ função de Zariski fechada e sobrejetora, de modo que i e j são compatíveis. Se X é completa, então X^* é completa.

Referência: A Proposição 10.1 de [Hrushovski, Zilber], para a qual há uma demonstração e um outro roteiro.

Essa proposição permite obter uma geometria de Zariski X^*, a partir de certas condições iniciais, que não é interpretável em nenhum corpo algebricamente fechado. É o que mostra a demonstração do Teorema C nas páginas 54 e 55.

7.6. Generalização de Hrushovski

Para provar a Conjectura de Mordell–Lang, o artigo [Hrushovski] adequa o estudo das geometrias de Zariski. Apresentamos aqui suas modificações.

Suponha T uma teoria completa, estável e com eliminação de quantificadores de uma linguagem L com um modelo $\mathfrak{A}$ e $\Phi(v)$ um conjunto de fórmulas de $\mathrm{L}(A)$ com uma única variável livre. Considere $P = \Phi(\mathfrak{A}) = \bigcap_{\phi\in\Phi} \phi(\mathfrak{A})$ o "conjunto-solução" de Φ. Pelos próximos poucos parágrafos, chamaremos P de *tipo*, como Hrushovski; corresponde de fato ao conjunto de realizações de um tipo incompleto. Se D é um subconjunto definível de A, dizemos que $D \cap P$ é um *subconjunto definível de* P, ou seja, trabalhamos com os definíveis em P.

Definição 7.6.1. P é *minimal* se todo seu subconjunto definível for finito ou cofinito.

P é *pluriminimal* se é união finita de tipos minimais.

P é *semi-(pluri)minimal* se existem um tipo (pluri)minimal Q e um conjunto finito F de modo que $P \subseteq \mathrm{acl}(Q \cup F)$.

Definição 7.6.2. Suponha que P é minimal. Dizemos que um subconjunto definível de P^n é *fechado* se é intersecção de P com um conjunto definido por uma fórmula sem quantificadores *positiva*, isto é, formada a partir de fórmulas atômicas com apenas conjunções e disjunções. Chamamos P um *tipo de Zariski* se

(i) Todo fechado em P^n é união finita de fechados irredutíveis.

(ii) Se $X \subset Y$ são fechados de P^n, com inclusão própria, e Y é irredutível, então $\dim X < \dim Y$.

(iii) Se X é um fechado irredutível de P^n, $\dim X = m$ e $Y = \{x \in P^n \mid x_i = x_j\}$, então $\dim W \geqslant m - 1$ para toda componente irredutível W de $X \cap Y$.

A Observação 2.4 de [Hrushovski] afirma que, sob essas condições, a coleção de fechados de P^n define uma topologia noetheriana e que a dimensão de um fechado nesta topologia iguala seu posto. Há um resquício de eliminação de quantificadores: para cada definível Y, existe um fechado F contido propriamente em $\mathrm{cl}(Y)$ tal que $Y - F = \mathrm{cl}(Y) - F$.

Na página 120 de [Marker A], há um exemplo de que P e seus fechados podem ***não*** ser uma geometria de Zariski.

Este é o resultado principal de nosso sumário:

Teorema 7.6.3. Suponha que P é um tipo de Zariski minimal, mas não localmente modular. Então T interpreta um corpo F, com subcorpos definíveis F_α tais que $\bigcap_\alpha F_\alpha$ é minimal e não-ortogonal a P.

Referência: O Lema 2.5 de [Hrushovski]. Note que esse resultado, quando P é "conjunto-solução" de uma única fórmula fortemente minimal, é demonstrado em [Hrushovski, Zilber] pelo Teorema B, mas a prova é idêntica. [Hrushovski] mostra na Item 2.20, pág. 667, como adaptar a Seção 6 de [Hrushovski, Zilber] adequadamente.

8
Duas classes de corpos

Este capítulo introduz duas classes de corpos que são utilizadas na demonstração modelo-teórica da Conjectura de Mordell–Lang: os corpos diferencialmente fechados e os corpos separavelmente fechados, de característica 0 e positiva respectivamente. Embora essas classes tenham interesse intrínseco em Álgebra e em Teoria dos Modelos, restringiremo-nos a expor o material necessário para nosso uso. Novamente, sugerimos que sejam exploradas com os merecidos detalhes em dissertações específicas.

A Seção A.5 do Apêndice de [Hodges] apresenta resultados da Teoria dos Modelos em diversas teorias de corpos. Evidentemente, já estudamos a linguagem dos corpos e ACF na Seção 1.2.

Atentamos para o fato de que, em muitas ocasiões, a linguagem apropriada é diferente, de modo que os raciocínios para ACF não se transferem imediatamente. É o caso dos corpos diferencialmente fechados, em que há um novo operador δ.

Este capítulo não é necessário para a apresentação da Conjectura de Mordell–Lang e seu enunciado modelo-teórico.

8.1. Corpos diferencialmente fechados

Exporemos sem pré-requesitos o que são os corpos diferenciais e diferencialmente fechados, porque não é um assunto estudado em nossos cursos de graduação ou pós-graduação principais.

Como referências, indicamos E. R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, 1973, I. Kaplansky, *An Introduction to Differential Algebra*, 2ª edição, Hermann, 1976, e o capítulo de C. Wood, *Differentially closed fields*, in [MTAG], p. 129–141.

Trabalharemos com a hipótese de característica 0, porque é o contexto em que esses corpos surgirão, e a teoria não é particularmente afinada para característica positiva.

À linguagem dos anéis, acrescenta-se um operador unário δ, chamado *derivação*: a teoria dos *anéis diferenciais* é obtida somando-se aos axiomas de anel os fechos das fórmulas $\delta(f + g) = \delta(f) + \delta(g)$; $\delta(fg) = \delta(f)g + f\delta(g)$. Chame $\delta(f)$ a *derivada* de f: a analogia com derivadas elementares é proposital.

Novamente, introduzimos a abreviatura padrão $\delta^n(t)$, para t termo e $n \in \mathbb{N}$. Se $n = 0$, $\delta^n(t)$ é o próprio termo t; se $n > 0$, $\delta^n(t)$ abrevia $\delta(\delta^{n-1}(t))$.

Atenção: acompanhando [MTAG], quando tratamos de corpos usamos o adjetivo "definível" para conjuntos definíveis na linguagem dos corpos e "δ-definível" na linguagem com derivação.

Sejam R um anel com unidade, $f, g \in R$ e uma derivação δ em R. Vemos que:

(i) $\delta(0) = 0 = \delta(1)$, pois $\delta(0) = \delta(0+0) = \delta(0) + \delta(0)$ e $\delta(1) = \delta(1.1) = \delta(1)1 + 1\delta(1)$.

(ii) $\delta(-f) = -\delta(f)$ e, caso R seja um corpo e $g \neq 0$, $\delta(g^{-1}) = -\delta(g)/g^2$. Temos, de fato, $\delta(f) + \delta(-f) = \delta(f + (-f)) = \delta(0) = 0$ e $\delta(g^{-1})g + g^{-1}\delta(g) = \delta(g^{-1}g) = \delta(1) = 0$. Desse modo, $\delta(\frac{f}{g}) = \delta(fg^{-1}) = \frac{\delta(f)g - f\delta(g)}{g^2}$.

(iii) Uma *constante* de R é um elemento cuja derivada seja 0. O conjunto de constantes é um subanel de R: de fato, vimos em (i) que 0 e 1 são constantes; a própria definição de δ implica fechamento sob $+$ e $.$, enquanto o item (ii) implica fechamento sob $-$. Caso R seja um corpo, o conjunto das constantes também é um subcorpo, pois é fechado sob $^{-1}$.

A essa altura, lembramos o exemplo tradicional: a derivação elementar em um anel de polinômios de uma variável x, que ao polinômio $\sum_{i=0}^{n} a_i x^i$ associa $\sum_{i=1}^{n} i a_i x^{i-1}$, é realmente uma derivação.

Exemplo 8.1.1. Suponha K um corpo qualquer de característica 0. Trabalharemos com os *corpos de funções racionais*, cujos elementos são quocientes de polinômios.

Lembramos que, inicialmente, o quociente de polinômios não é definido em um anel de polinômios $K[x]$. O símbolo f/g, para $f, g \in K[x]$, não necessariamente representa um polinômio; o quociente $f(a)/g(a)$ não está definido se a for raiz de g. Contudo, esse anel certamente possui um corpo de frações, notadamente o conjunto das classes de equivalência de pares (f, g) representados f/g e identificados assim: $f/g = p/q \Leftrightarrow fq = pg$. Esse corpo é indicado $K(x)$.

Sendo $\delta : K[x] \to K[x]$ qualquer derivação, estendemo-la à operação $\delta : K(x) \to K(x)$, $\delta(f/g) = \frac{g\delta(f) - \delta(g)f}{g^2}$, como é sugerido pelo item (ii) acima. Verifica-se que δ está bem-definida, realmente estende a derivação original e é uma derivação.

Assuma agora que R é comutativo, com uma derivação δ. Podemos construir um outro anel diferencial $R\{x\}$, deste modo: imitando a definição de um anel de polinômios de infinitas variáveis, consideramos um anel de polinômios nas variáveis $\delta^n(x)$, $n \in \mathbb{N}$, em que $\delta^n(x)$ é apenas um símbolo. Um tal polinômio tem a forma

$$\sum_{i=0}^{k_0} a_{0i}x^i + \sum_{i=0}^{k_1} a_{1i}(\delta(x))^i + \ldots + \sum_{i=0}^{k_n} a_{ni}(\delta^n(x))^i \, .$$

Para $f \in R\{x\}$ não-nulo, seja ord(f) a *ordem* de f, isto é, o maior natural n tal que uma potência não-nula de $\delta^n(x)$ ocorre em f com coeficiente não-nulo, ou equivalentemente o menor n tal que $f \in R[x, \ldots, \delta^n(x)]$. Desse modo, têm ordem 0 os polinômios não-constantes de $R[x]$; defina como -1 a ordem de cada elemento não-nulo de R. Podemos naturalmente estender a derivação δ a todo $R\{x\}$ com $\delta(\delta^n(x)) = \delta^{n+1}(x)$.

Suponha agora K um corpo diferencial com uma derivação δ.

Definição 8.1.2. (i) Um ideal I de $K\{x\}$ é *diferencial* se $\delta(f) \in I$ para todo $f \in I$.

(ii) Suponha $K \subseteq L$, em que L é um corpo diferencial extensão de K cuja derivação estende δ, e $a \in L$. Diz-se que a é *diferencialmente algébrico* sobre K se existe $f \in K\{x\}$ não-nulo tal que $f(a) = 0$; caso contrário a *diferencialmente transcendente*.

(iii) Suponha $K \subseteq L$ como acima e $a \in L$. Indicamos o menor subcorpo de L que contém a e K e é fechado sob a derivação de L como $K\langle a\rangle$.

Proposição 8.1.3. Suponha $K \subseteq L$, em que L é um corpo diferencial extensão de K cuja derivação estende δ.

(i) Suponha que $f \in K\{x\}$ seja não-nulo, com ordem no máximo m. Suponha $a, b \in L$ tais que $f(a) = f(b) = 0$, $\{a, \ldots, a^{m-1}\}$ e $\{b, \ldots, b^{m-1}\}$ sejam cada um conjuntos algebricamente independentes sobre K, e $g(a) \neq 0$, $g(b) \neq 0$ para qualquer g de ordem m de grau menor em $\delta^m(x)$. Então $K\langle a\rangle$ e $K\langle b\rangle$ são isomorfos sobre K como corpos diferenciais.

(ii) Se $a \in L$ é algébrico sobre K, então existe $f \in K\{x\}$ não-nulo tal que $f(a) = 0$ de ordem mínima. Pode-se escolher f de modo que, se a mesma asserção vale para $b \in L$, então $K\langle a\rangle$ e $K\langle b\rangle$ são isomorfos sobre K como corpos diferenciais.

(iii) Dado $f \in K\{x\}$, existem L e $a \in L$ como na hipótese tais que $f(a) = 0$ e $g(a) \neq 0$ para todo $g \in K\{x\}$ não-nulo com ord$(f) >$ ord(g).

Referência: A Proposição 4.3.30 de [Marker].

Procuramos por corpos em que as "equações diferenciais" tenham solução. Um corpo diferencial K é chamado *diferencialmente fechado* se para todos $f, g \in K\{x\}$ não-nulos com ord$(f) >$ ord(g) existe $a \in K$ tal que $f(a) = 0$ e $g(a) \neq 0$.

Iterando o resultado (iii) da proposição, obtemos primeiramente uma extensão de K em que essa propriedade vale para todos os polinômios de $K\{x\}$. Novamente procedendo por indução e construindo uma cadeia de corpos, concluímos que existe uma extensão de K que é diferencialmente fechada.

Observamos que se axiomatiza a teoria DCF_0 dos corpos diferencialmente fechados (*differentially closed fields*, em inglês): basta acrescentar aos axiomas de corpo de característica 0, para $m > n$ e k, l quaisquer, as sentenças que afirmam que, para todos a_{ji} com $0 \leqslant j \leqslant m$, $0 \leqslant i \leqslant k$ com algum $a_{mi} = 1$ e para todos b_{ji} com $0 \leqslant j \leqslant n$, $0 \leqslant i \leqslant l$ com algum $b_{ni} = 1$ existe x tal que

$$\sum_{j=0}^{m}\sum_{i=0}^{k} a_{ji}(\delta^j(x))^i = 0\,, \quad \sum_{j=0}^{n}\sum_{i=0}^{l} b_{ji}(\delta^j(x))^i \neq 0$$

(As restrições $\bigvee_{i=0}^{k}(a_{mi} = 1)$ e $\bigvee_{i=0}^{l}(b_{ni} = 1)$ garantem que os polinômios têm ordens m e n respectivamente.), sendo uma pequena correção necessária para o caso $n = -1$, em que só se escreve o primeiro polinômio. Vimos acima que realmente DCF_0 tem modelos, bastando considerar um corpo diferencial qualquer K.

Teorema 8.1.4. DCF_0 contém ACF_0 e admite eliminação de quantificadores.

Referências: Quando $f \in K\{x\}$ tem $\text{ord}(f) = 0$, vemos que f é simplesmente um polinômio de $K[x]$ não-constante, ou seja, grau ao menos 1. A respeito da eliminação de quantificadores, que se dá na linguagem com o operador δ, veja o Teorema 4.3.32 de [Marker] ou o Teorema 6.16 de [Poizat 1].

Suponha agora $K \subseteq L$ como anteriormente, mas com $L \models DCF_0$.

Podemos considerar também o anel $K\{x_1, \ldots, x_n\}$, obtido do mesmo modo que $K\{x\}$ mas com n variáveis "básicas" e independentes: a derivada de $\delta^m(x_i)$ é $\delta^{m+1}(x_i)$. A definição de ideal diferencial é a mesma.

Veremos algumas generalizações de resultados clássicos e de associações que trabalhamos para a teoria ACF:

Fato 8.1.5. Dado $p \in S_n^L(K)$, o conjunto $\varphi(p) = \{f \in K\{x_1, \ldots, x_n\} \mid (f(v) = 0) \in p(v)\}$ é um ideal próprio, diferencial e primo. A função φ é uma bijeção entre $S_n^L(K)$ e o conjunto desses ideais.

Teorema 8.1.6 (Base de Ritt–Raudenbusch). Toda cadeia crescente de ideais diferenciais e radicais de $K\{x_1, \ldots, x_n\}$ estaciona (em "comprimento" finito).

Referência: O Teorema 7.1 do livro de Kaplansky que mencionamos no início da seção.

De modo análogo ao Exemplo 2.3.8,

Corolário 8.1.7. DCF_0 é ω-estável.

Corolário 8.1.8. Sendo K diferencialmente fechado, define-se um subconjunto *fechado de Kolchin* de K^n como uma união finita de conjuntos de raízes comuns de um número finito de polinômios de $K\{x_1, \ldots, x_n\}$. Então os complementos dos conjuntos fechados formam uma topologia noetheriana, chamada *de Kolchin*.

Teorema 8.1.9 (*Nullstellensatz* diferencial). Suponha $K \models DCF_0$. Sejam P um ideal diferencial primo e p um polinômio de $K\{x_1, \ldots, x_n\}$. Suponha que todo $a \in K^n$ que seja raiz de todo polinômio em P é também raiz de p. Então $p \in P$.

Definição 8.1.10. Suponha que $K \subseteq L$ sejam ambos diferencialmente fechados. Diz-se que L é um *fecho diferencial* de K se, para toda extensão diferencial F, diferencialmente fechada, existe uma imersão de L em F fixando os elementos de K.

Os fechos diferenciais sempre existem, como mostra o Teorema de Blum, Teorema 41.3 de G. E. Sacks, *Saturated Model Theory*, W. A. Benjamin, Inc., 1972. Uma "unicidade" é exposta no Teorema 6.4.10 de [Marker].

8.2. Corpos separavelmente fechados

Estes corpos serão necessários quando a característica é positiva: fixamos agora um primo $p > 0$. Também é adequado expor este desenvolvimento em um modelo monstro: um corpo algebricamente fechado de alta cardinalidade.

O artigo fundamental desta área é Y. Ershov, *Fields with a solvable theory*, Sov. Math. Dokl. (tradução AMS) vol. 8, no. 3, 1967, p. 575-576. A referência para nosso estudo é o capítulo de F. Delon, *Separably closed fields*, in [MTAG], p. 143–176.

Recordamos que um polinômio irredutível é *separável* se todas as suas raízes são distintas. Um elemento x algébrico sobre um corpo K é dito *separável sobre* K se seu polinômio minimal sobre K é separável.

Seja K^s o conjunto dos elementos separáveis sobre K: trata-se do *fecho separável* de K. Diz-se que K é *separavelmente fechado* se $K = K^s$.

O *grau de imperfeição* de K ou *invariante de Ershov* é um número natural ou o infinito ∞, indicado ν, definido de modo que $\nu \in \mathbb{N} \Leftrightarrow [K : K^p] < \omega$ e, nesse caso, $p^\nu = [K : K^p]$. Assumiremos sempre que ν é finito.

A teoria $SCF_{p,\nu}$ dos corpos separavelmente fechados (*separably closed fields*, em inglês) de característica p e grau ν é completa, como mostra o Teorema 2.1 do capítulo de Delon.

9
A Conjectura de Mordell–Lang

Concluímos nosso texto expondo a Conjectura de Mordell–Lang, o enunciado equivalente natural em Estabilidade e a demonstração de Hrushovski.

Não trabalharemos a respeito de estimativas, que são um aspecto do problema de finitude de soluções. Mencionamos apenas que a Compacidade modelo-teórica já fornece automaticamente estimativas uniformes, mas pobres. Maior precisão é obtida na Seção 6 de [Hrushovski].

Podemos supor todos os corpos algebricamente fechados, com exceção de $\mathbb{Q}$, porque basta sempre considerar seus fechos algébricos para obter os enunciados gerais.

Todas as curvas de que tratarmos são suaves por hipótese.

9.1. Diversas conjecturas

A Conjectura de Mordell–Lang, como trataremos aqui, é o enunciado mais abrangente de uma cadeia de conjecturas iniciada por Louis Joel Mordell em 1922 e desenvolvida por Serge Lang nos anos 60, mas estendida e demonstrada por Ehud Hrushovski em 1996 após uma década de aproximações.

Esta seção apresenta essa cadeia de conjecturas, com comentários históricos e matemáticos derivados de [Hindry], [Pillay 97] e [Lang 2], para cujas bibliografias remetemos o leitor interessado nos artigos originais.

Consideremos uma curva projetiva suave C definida em um corpo de números algebricamente fechado K. Há três possibilidades para o genus g de C:

Se $g = 0$, então $C(\mathbb{Q}) = \emptyset$ ou todas as soluções *exceto um número finito* são parametrizadas por funções racionais. Também sabemos que C é isomorfa a $\mathbb{P}^1$, de modo que $C(K)$ é igual a todo $\mathbb{P}^1(K)$.

Se $g = 1$, então $C(\mathbb{Q}) = \emptyset$ ou C é uma curva elíptica. O Teorema de Mordell–Weil afirma que, neste caso, $C(K)$ é um grupo abeliano finitamente gerado.

Nesses dois casos, é freqüente que $C(K)$ seja infinito, e isso será sempre verdade para $C(L)$, em que L é alguma extensão finita de K.

Se $g \geqslant 2$, Mordell conjecturou que a situação é diferente:

(M) Se C é uma curva de genus $\geqslant 2$ definida sobre um corpo numérico K, então $C(K)$ é finito.

A conjectura (M) foi provada por Faltings em 1983.

Suponha agora $A = J(C)$ a jacobiana de C. Com C imerso em A, temos $C(\mathbb{Q}) = C \cap A(\mathbb{Q})$. Seja Γ um subgrupo finitamente gerado de A. Assumindo (M), $\Gamma \cap C$ é finito. O Teorema de Mordell–Weil mostra que (M) equivale a este enunciado: "Se X é uma curva em uma variedade abeliana A e Γ é um subgrupo finitamente gerado de A, então $\Gamma \cap X$ é finito ou X é transladado de uma curva elíptica."

Associa-se a esse enunciado a Conjectura de Manin–Mumford:

(MM) A intersecção de X com o conjunto dos pontos de torsão de $J(X)$ é finita, ou a intersecção de X com o conjuntos dos pontos de uma variedade abeliana A em que X esteja imerso é finita, exceto se X é transladado de uma curva elíptica.

Em 1960, Lang considerou uma situação análoga para corpos de funções, chamada *relativa*:

(L) Sejam K um corpo de funções sobre um corpo K_0 de característica 0 e C uma curva sobre K de genus $\geqslant 2$. Então $C(K)$ é finito ou C é isomorfa a uma curva C_0 definida sobre K_0 e todos os pontos de $C(K)$ *exceto um número finito* correspondem a pontos de $C_0(K_0)$ sob esse isomorfismo.

A demonstração de Manin em 1963 teve que ser corrigida posteriormente, mas é importante notar que já fazia uso de corpos diferencialmente fechados.

A última conjectura de Lang tomou forma em 1965:

(ML) Sejam S uma variedade semi-abeliana definida sobre um corpo de característica 0, X uma subvariedade de S e Γ um subgrupo de gradação finita de S. Então $X \cap \Gamma$ é uma união finita de transladados de subgrupos de S.

A demonstração desse enunciado para Γ finitamente gerado é devida a Vojta em 1996 e a redução a esse caso havia sido feita por McQuillan no ano anterior. O caso abeliano e de grupos finitamente gerados data de 1994 por Faltings. Quando S é abeliana e Γ é seu grupo de pontos de torsão, o enunciado corresponde à Conjectura de Manin–Mumford, demonstrada por Raynaud e estendida por Hindry.

Estamos em posição de decifrar a fórmula que ilustra a capa de [MTAG]. Pela Proposição 6.3.3, o enunciado (ML) afirma que existem $\gamma_1, \ldots, \gamma_m \in \Gamma$ e subvariedades abelianas de A tais que $\gamma_i + B_i \subseteq X$ e

$$\Gamma \cap X(K) = \bigcup_{i=1}^{m} (\gamma_i + B_i(K) \cap \Gamma) .$$

Argumentemos que (ML) implica (M). Seguindo a nomenclatura em (M), seja A a variedade jacobiana de C, também definida sobre K_0. Pelo Teorema de Mordell–Weil, $A(K_0)$ é finitamente gerado. Ora, $C(K_0) = C \cap A(K_0)$, de modo que (ML) implica que o fecho de $C(K)$ é uma união finita de transladados de subvariedades abelianas de A. Se todas forem triviais, $C(K)$ é finito. Se não, como a dimensão de C é 1, o próprio $C(K)$ é um desses transladados e, portanto, tem genus 1, contradição.

Observemos que, com esses enunciados, (M) e (ML) falham em característica $p > 0$. Suponha X uma curva de genus $\geqslant 2$ sobre o corpo primo F_p de p elementos e A sua jacobiana. Sejam K_0 o fecho algébrico de F_p, t um ponto K_0-genérico de X, $K = K_0(t)$ e Γ o subgrupo de $A(K)$ gerado por $\{t^{p^n} \mid n \in \mathbb{N}\}$. Pelo Teorema de Lang–Nerón, Γ é finitamente gerado e $X \cap \Gamma$ não pode ser união finita de transladados. Analogamente, $X(K) - X(K_0)$ é finito.

Uma versão possível, devida independentemente a Grauert e Samuel em 1965, tira a condição problemática:

(GS) Se K_0 é um corpo algebricamente fechado de característica $p > 0$, K é uma extensão finitamente gerada de K_0 e C é uma curva de genus $\geqslant 2$ definida sobre K_0 que não é fracamente isomorfa a uma curva sobre K_0, então $C(K)$ é finito.

Para enunciar a versão proposta e demonstrada em [Hrushovski], devemos fazer a convenção usual de que os objetos que buscamos são "especiais":

Definição 9.1.1. Suponha que $K_0 \subseteq K$ são corpos e S é uma variedade semi-abeliana definida sobre K. Uma subvariedade X de S é *especial com respeito a* K_0 se existem um subgrupo algébrico S_1 de S, uma variedade semi-abeliana S_0 definida sobre K_0, uma subvariedade X_0 de S_0 definida sobre K_0 e um homomorfismo racional $h : S_1 \to S_0$ de grupos algébricos tal que $X = h^{-1}[X_0] + c$ para algum $c \in S$.

Em particular, uma subvariedade especial é um transladado de um subgrupo.

(H) Sejam S uma variedade semi-abeliana definida sobre um corpo de característica *qualquer*, X uma subvariedade de S e Γ um subgrupo de gradação finita de S. Então existem subvariedades especiais $X_1, \ldots, X_n$ de S tais que $X \cap \Gamma \subseteq X_1 \cup \ldots \cup X_n \subseteq X$.

Um caso particular é devido a Buium. O enunciado para característica positiva é devido a Abramovich e Voloch; frisamos que, anteriormente à demonstração de Hrushovski, a validade de qualquer enunciado geral em característica positiva era desconhecido.

Novamente, observa-se que (H) implica (ML).

9.2. O enunciado modelo-teórico

Esta seção não é pré-requesito para a próxima: devotamo-la a estudar o capítulo [Pillay B], que demonstra a equivalência dos enunciados (ML) e

> (P) Sejam K um corpo algebricamente fechado de característica 0, S uma variedade semi-abeliana sobre K e Γ um subgrupo de gradação finita de S. Então $Th(K, \Gamma, (a)_{a \in K})$ é estável e Γ é um-baseado.

cujo ambiente natural é a Teoria dos Modelos. Observamos que a estrutura $(K, \Gamma, (a)_{a \in K})$ constitui-se do corpo K, para o qual subentende-se a linguagem dos anéis com unidade, de Γ subgrupo de S, por sua vez contido em K^n, ou seja, Γ é uma relação n-ária sobre K, e dos elementos de K como constantes.

Diferimos de [Pillay B] nesta

Definição 9.2.1. Sejam K corpo algebricamente fechado, G grupo algébrico comutativo sobre K e Γ um subgrupo qualquer de G. A tripla (K, G, Γ) é do *tipo de Lang* se, para toda subvariedade X de G sobre K, $X \cap \Gamma$ é união finita de transladados de subgrupos de G.

Assim, (ML) diz que, se K tem característica 0 e Γ é um subgrupo de gradação finita de S variedade semi-abeliana sobre K, então (K, S, Γ) é do tipo de Lang. Provaremos o

Teorema 9.2.2 (Pillay *et al.*). Sejam K corpo algebricamente fechado, G grupo algébrico comutativo sobre K e Γ subgrupo de G. Então (K, G, Γ) é do tipo de Lang se e somente se $Th(K, \Gamma, (a)_{a \in K})$ é estável e Γ é um-baseado.

Não aplicaremos a delimitação usual *Demonstração*–QED, porque o raciocínio conterá resultados intermerdiários de destaque.

Inicialmente provamos a implicação inversa. Suponha X subvariedade de S^n. Então $X \cap \Gamma^n$ é definível na estrutura $(K, \Gamma, (a)_{a \in K})$. Por hipótese e a Proposição 5.4.4, $X \cap \Gamma$ é combinação booleana finita de transladados. Mostra-se que o fecho de Zariski (em um grupo algébrico comutativo) de uma tal combinação é uma união finita de transladados laterais de subgrupos algébricos, bastando aplicar a Proposição 6.3.3.

Dedicamo-nos agora à implicação direta. Sejam $\mathfrak{M} = (K, S, \Gamma, (a)_{a\in K})$, $T = Th(\mathfrak{M})$, $\mathbf{\Gamma} = (\Gamma, (X \cap \Gamma^n)_X)$ em que X percorre os subconjuntos de S^n definíveis com parâmetros em K. Assuma (K, G, Γ) do tipo de Lang.

Lema 9.2.3. $T_0 = Th(\mathbf{\Gamma})$ é um-baseada.

Demonstração: Qualquer subconjunto X de G definível sobre K é combinação booleana finita de subvariedades irredutíveis X_i de G. Então $X \cap \Gamma$ é uma combinação finita dos $X_i \cap \Gamma$. Como (K, G, Γ) é do tipo de Lang, $X_i \cap \Gamma = \bigcup_j (C_{ij} \cap \Gamma)$ em que C_{ij} é um transladado de um subgrupo algébrico G_{ij} de G. Assim, cada definível em $\mathbf{\Gamma}$ é definível no reduto $\mathbf{\Gamma}_0 = (\Gamma, (B \cap \Gamma)_B)$ em que B percorre os subgrupos algébricos de G. Sabe-se que toda fórmula de $Th(\mathbf{\Gamma}_0)$ equivale a uma combinação booleana de fórmulas primitivas positivas. Em particular, todo conjunto definível é combinação booleana de transladados. Então $Th(\mathbf{\Gamma}_0)$ e também $Th(\mathbf{\Gamma})$ é estável e um-baseada.

QED

Seja $\kappa > |T|$ tal que T_0 é κ-estável. Seja $\mathfrak{N}$ modelo de T saturado com $|N| \geqslant \kappa$. Então $\mathfrak{M} \prec \mathfrak{N} = (K_1, G_1, \Gamma_1, (a)_{a\in K})$. Tome $\mathbf{\Gamma}_1 = (\Gamma_1, (Y \cap \Gamma_1)_Y)$ em que Y percorre os subconjuntos de $G(K_1)$ definíveis com parâmetros em K. Então $\mathbf{\Gamma} \prec \mathbf{\Gamma}_1$.

Seja $\mathrm{acl}_f(\cdot)$ o fecho algébrico como corpo (*field*).

Lema 9.2.4. Se $B \subseteq N$, $|B| \leqslant \kappa$, então existe $C \subseteq \Gamma_1$, $|C| \leqslant \kappa$, tal que, para todos $a_1, a_2 \in \Gamma_1$ com mesmo tipo sobre C em $\mathbf{\Gamma}_1$, existe $f : \mathrm{acl}_f(B \cup K \cup \Gamma_1) \to \mathrm{acl}_f(B \cup K \cup \Gamma_1)$ satisfazendo

(i) f fixa os elementos de B, K, C.

(ii) $f|_{\Gamma_1}$ é automorfismo de $\mathbf{\Gamma}_1$.

(iii) f é (parcial) elementar em $(K_1, G_1, (a)_{a\in K})$.

(iv) $f(a_1) = a_2$.

(v) Para todos $c, d \in N - \mathrm{acl}_f(B \cup K \cup \Gamma_1)$ existe automorfismo g de $\mathfrak{N}$ que estende f e $g(c) = d$.

Demonstração: Tome $B' = B \cup K$. Para cada upla b de B', seja C_b um subconjunto finito de Γ_1 tal que o tipo de b sobre Γ_1 em $(K_1, G_1, (a)_{a\in K})$ é definível sobre C_b (existe pois $Th(K_1, G_1)$ é ω-estável). Seja $C = \bigcup_b C_b$, com $|C| \leqslant \kappa$. Sejam a_1, a_2 como no enunciado: tome f_1 automorfismo de $\mathbf{\Gamma}_1$ que fixa os elementos de C e $f_1(a_1) = a_2$.

Verifiquemos que, para qualquer upla b de B' e qualquer upla a de Γ_1, (b, a) e $(b, f_1(a))$ têm o mesmo tipo em $(K_1, G_1, (a)_{a\in K})$. Suponha $\phi(x, y)$ fórmula da linguagem de $(K_1, G_1, (a)_{a\in K})$. Existem upla c de C e fórmula $\psi(y, z)$ dessa linguagem tais que $K_1 \models \phi(b, a) \Leftrightarrow K_1 \models \psi(a, c)$. Mas $\psi \cap \Gamma_1$ é $\emptyset$-definível em $\mathbf{\Gamma}_1$. Como f_1 é elementar em $\mathbf{\Gamma}_1$, temos $K_1 \models \psi(a, c) \Leftrightarrow K_1 \models \psi(f_1(a), c)$, donde $K_1 \models \phi(b, a) \Leftrightarrow K_1 \models \phi(b, f_1(a))$, como desejado.

Seja $f_2 : B' \cup \Gamma_1 \to B' \cup \Gamma_1$ que estende f_1 e é a identidade em B'. Então f_2 é elementar em $(K_1, G_1, (a)_{a\in K})$. Seja f extensão de f_2 a uma permutação elementar (em $(K_1, G_1, (a)_{a\in K})$) de $\mathrm{acl}_f(B' \cup \Gamma_1)$. Então f satisfaz (i)–(iv). Dados $c, d \in N - \mathrm{acl}_f(B' \cup \Gamma_1)$, f estende-se a um automorfismo g de $(K_1, G_1, (a)_{a\in K})$ com $g(c) = d$. Como g fixa Γ_1, é automorfismo de $\mathfrak{N}$. QED

Como T_0 é κ-estável, também o é T. Se $\mathfrak{N} = (K_1, G_1, \Gamma, (a)_{a\in K}) \models T$, então qualquer subconjunto de Γ_1^n definível em $\mathfrak{N}$ é definível em $\mathbf{\Gamma}_1$. Do fato e do primeiro lema, Γ é um-baseado para T. Isso conclui a demonstração do teorema.

A verificação da Conjectura de Lang produz, então, uma coleção de teorias estáveis $Th(K, \Gamma, (a)_{a\in K})$. [Pillay B] credita esta conseqüência da demonstração a uma observação de Poizat:

Proposição 9.2.5. Suponha D conjunto fortemente minimal, Γ subconjunto arbitrário de D^n. Seja $\mathbf{\Gamma} = (\Gamma, (X \cap \Gamma^m)_X)$ em que X percorre os subconjuntos definíveis de D^{nm}, qualquer $m \in \mathbb{N}$. Seja $\mathbf{\Gamma}' = (\Gamma, (Y)_Y)$ em que Y percorre os subconjuntos definíveis de Γ^m em (D, Γ), qualquer $m \in \mathbb{N}$. Então $\mathbf{\Gamma}$ e $\mathbf{\Gamma}'$ têm as mesmas relações $\emptyset$-definíveis.

9.3. Demonstração do enunciado (H)

Esta seção demonstra o enunciado (H) da Conjectura de Mordell Lang. Nossa apresentação combina o artigo original [Hrushovski] e a exposição em [Bouscaren B], mas há também um roteiro mínimo no final de [Pillay 97].

A demonstração em si é feita para um caso extremamente particular, ao qual se reduz previamente o enunciado geral. Desse modo, como na seção anterior, os raciocínios não estão delimitados pelo usual *Demonstração*–QED.

Seguiremos a linha original de [Hrushovski], ao apresentar paralelamente as demonstrações para os casos de característica 0 e positiva, já que muitos enunciados são os mesmos quando as hipóteses são adequadas. Em [Bouscaren B], as variedades estudadas são abelianas e os casos são tratados isoladamente: o de característica 0 é apresentado em maiores detalhes e o de característica positiva é posteriormente roteirizado.

A primeira redução consiste em considerar, no enunciado (H), o fecho de $X \cap \Gamma$ escrito como união de suas componentes irredutíveis: $\mathrm{cl}(X \cap \Gamma) = X_1 \cup$

$\ldots \cup X_n$, em que cada X_i é um fechado irredutível, portanto subvariedade. Note que $\mathrm{cl}(X \cap \Gamma) \cap \Gamma \subseteq \mathrm{cl}(X \cap \Gamma)$, enquanto de $X \cap \Gamma \subseteq \mathrm{cl}(X \cap \Gamma) \cap \Gamma$ vem $\mathrm{cl}(X \cap \Gamma) \subseteq \mathrm{cl}(\mathrm{cl}(X \cap \Gamma) \cap \Gamma)$, concluindo-se que $\mathrm{cl}(\mathrm{cl}(X \cap \Gamma) \cap \Gamma) = \mathrm{cl}(X \cap \Gamma)$. Assim,

$$\mathrm{cl}(X_1 \cap \Gamma) \cup \ldots \cup \mathrm{cl}(X_k \cap \Gamma) = \mathrm{cl}((X_1 \cup \ldots \cup X_k) \cap \Gamma) = \mathrm{cl}(X \cap \Gamma),$$

mas cada $\mathrm{cl}(X_i \cap \Gamma) \subseteq X_i$. Suponha que $\mathrm{cl}(X_i \cap \Gamma)$ esteja propriamente contido em X_i: então $X_i - \mathrm{cl}(X_i \cap \Gamma)$ é um aberto não-vazio de X_i, portanto denso e seu fecho é X_i. Porém $X_i - \mathrm{cl}(X_i \cap \Gamma) \subseteq \mathrm{cl}(X \cap \Gamma) = \mathrm{cl}(X_1 \cap \Gamma) \cup \ldots \cup \mathrm{cl}(X_k \cap \Gamma)$, de modo que $X_i - \mathrm{cl}(X_i \cap \Gamma) \subseteq \bigcup_{j \neq i} \mathrm{cl}(X_j \cap \Gamma) \subseteq \bigcup_{j \neq i} X_j$ fechado. Tomando o fecho, obtemos $X_i \subseteq \bigcup_{j \neq i} X_j$ e então existe $j \neq i$ tal que $X_i \subseteq X_j$, contrariando o Fato 6.1.1. Desse modo, cada $\mathrm{cl}(X_i \cap \Gamma) = X_i$, ou seja, $X_i \cap \Gamma$ é denso em X_i. Como precisamos apenas que cada X_i seja especial para aplicar o Corolário 6.3.4, basta demonstrar o

Teorema 9.3.1 (Hrushovski). Sejam $K_0 \subseteq K$ corpos algebricamente fechados, S uma variedade semi-abeliana sobre K, X uma subvariedade de S e Γ um subgrupo de gradação finita de S. Suponha que $X \cap \Gamma$ é denso em X. Então X é especial com respeito a K_0.

Apresentamos agora uma redução devida a Buium. Tome S, X, K_0, Γ como neste enunciado e tome L uma extensão finitamente gerada de K_0 tal que S, X e um conjunto de geradores de Γ estão definidos sobre L.

Em característica p, $[L : L^p]$ é finito e $\bigcap_{n \in \mathbf{N}} L^{p^n} = K_0$, de modo que o mesmo vale para um fecho separável K de L. Tome $\Gamma_n = p^n S$, de modo que $\bigcap_{n \in \mathbf{N}} \Gamma_n$ tem dimensão finita. Então $\Gamma / p^n \Gamma$ é finito e Γ intersecta apenas um número finito de classes laterais de Γ_n, de modo que alguma classe lateral de Γ_n intersecta X em um conjunto denso.

Em característica 0, dotamos L de uma derivada para a qual K_0 é o corpo de constantes e tomamos K um fecho diferencial de L. Buium mostrou que existe um subgrupo de S de dimensão finita contendo Γ.

Adiantamo-nos e consideramos a Observação 5.8 de [Hrushovski], ou a Subseção 2.1 de [Bouscaren B]. Tomaremos K' uma extensão elementar $|K|^+$-grande de K e K'_0 o corpo de constantes de K' se a característica é 0 ou $K'_0 = \bigcap_{n \in \mathbf{N}} (K')^{p^n}$ se a característica é p. Temos $K_0 \subseteq K'_0$. Provaremos o teorema com K' e K'_0 em vez de K e K_0: existem S'_1 uma subvariedade grupo de $S' = S(K')$, uma variedade semi-abeliana S'_0 definida sobre K'_0, uma subvariedade X'_0 de S'_0 definida sobre K'_0 e um morfismo bijetor $h' : S'_1 \to S'$ tal que $X = a'_0 + (h')^{-1}[X'_0]$.

Verifiquemos que podemos voltar ao enunciado original com K e K_0. Como K é algebricamente fechado, por rigidez S_1' também é definida sobre K_0. A afirmação "h' é um morfismo bijetor de S_1' em S' com subvariedade X_0' definidos sobre K_0' tal que $X = a_0' + (h')^{-1}[X_0']$" corresponde a uma sentença com constantes em K' necessárias para definir h', S, B, X, lembrando que K_0' é definível em K'. Já que $K \prec K'$, podemos considerar as variedades e os morfismos definidos pelas fórmulas em K.

Notamos que K' é grande em um cardinal maior que o do conjunto de parâmetros necessários para definir todos esses conjuntos e funções.

Desse modo, é suficiente provar o

Teorema 9.3.2 (Hrushovski). Assuma tais condições para K, e K_0 o corpo de constantes de K se a característica for 0, ou $K_0 = \bigcap_{n\in\mathbf{N}} K^{p^n}$ se a característica for $p > 0$. Sejam S uma variedade semi-abeliana definida sobre K e X uma subvariedade de S. Seja Γ um subgrupo infinitamente definível de S de dimensão finita. Assuma $X \cap \Gamma$ denso em X. Então X é especial com respeito a K_0.

Trabalharemos agora sobre este enunciado, assumindo os lemas técnicos de [Hrushovski] que se fizerem necessários. Podemos assumir que X tem estabilizador finito, caso contrário quocientamos pela componente conexa do estabilizador. Seja A o subgrupo conexo maximal semi-pluriminimal de Γ. Por hipótese $X \cap \Gamma$ é denso em X. Tome Y um definível contido em $X \cap \Gamma$ tal que Y é denso em X e de posto e grau mínimos. Já que X é irredutível, se $Y = Y_1 \cup \ldots \cup Y_r$ então um dos Y_i tem que ser denso em X, concluindo-se que o grau de Y é 1. Além disso, se Y' é um subconjunto de Y de mesmo posto, então Y' é denso em X, já que seu complemento não pode ser.

Observe que, se translação por um elemento a estabiliza Y no sentido de $\mathrm{RM}(Y \cap (a+Y)) = \mathrm{RM}(Y)$, então o fecho de $Y \cap (a+Y)$ precisa ser X. Como $X \cap (a+X)$ é fechado e contém $Y \cap (a+Y)$, o elemento a estabiliza X como um conjunto. Então o estabilizador "posto" de Y está contido no estabilizador "conjunto" de X e é finito.

Portanto, um subconjunto de Y de mesmo posto está contido em um transladado $c + A$. Em particular, $(c + A) \cap X$ é denso em X. Substituindo X por $X - c$ e Γ por A, podemos assumir que Γ é semi-pluriminimal.

Escreva A como uma soma de subgrupos ortogonais A_i semi-minimais. Seja B a soma de todos os A_i não localmente modulares, e C a soma dos demais. Se A_i, A_j são não localmente modulares, então são não ortogonais a K_0, e portanto entre si, donde $i = j$. Então B é semi-pluriminimal. Y está contido em um transladado de B. Novamente por translação, podemos assumir que $Y \subseteq B$.

Seja G o fecho de B. Então G é uma subvariedade grupo de S, contendo X fecho de Y. Suponha que existem um grupo algébrico S_0 definido sobre K_0 e um homomorfismo racional bijetor $h : G \to S_0$ definida sobre K e $h[B] = S_0(K_0)$. Então S_0 é semi-abeliana. Seja X_0 o fecho de $h[Y]$. Já que $h[Y] \subseteq h[B] \subseteq S_0(K_0)$, temos X_0 definida sobre K_0. Claramente $h^{-1}[X_0]$ contém X. Já que h é bijetor, $h^{-1}(X_0) = X$.

Assim, basta mostrar que S_0 e h existem:

Proposição 9.3.3. Sejam S uma variedade semi-abeliana definida sobre K e A um subgrupo definível semi-minimal de S, denso em S. Então ou A é localmente modular ou existe um grupo algébrico H definido sobre K_0 e um homomorfismo racional bijetor $h : S \to H$ com $h[A] = H(K_0)$.

Demonstração: Assuma que A não é localmente modular. Existem um grupo algébrico H definido sobre K_0 e um homomorfismo de grupos definível e sobrejetor $h_1 : A \to H(K_0)$ com núcleo finito com, digamos, n elementos. Dado $y \in h_1[A]$, existe $x \in H$ com $y = h_1(x)$; defina $g_0(y) = nx$, bem-definido porque se $h_1(x) = h_1(x')$ então $x - x'$ está no núcleo de h_1 e $n(x - x') = 0$. Vemos que g_0 é um homomorfismo sobrejetor. Mas o conjunto dos pontos de n-torsão de H é finito, de modo que g_0 tem núcleo finito.

g_0 é uma função quase-racional. Já que $h_1[A]$ é denso em H, g_0 define um homomorfismo $g : H \to S$. Seja R o menor subgrupo fechado de H com H/R semi-abeliano. Então R está definido sobre K_0. H/R é fortemente rígido, donde $(\mathrm{Ker}g)/R$ está definido sobre K_0 e também $\mathrm{Ker}g$ está. Já que K_0 é algebricamente fechado, existe um grupo algébrico H' definido sobre K_0 e uma função sobrejetora quase-racional $f : H \to H'$ com núcleo $\mathrm{Ker}g$. Obtemos uma função quase-racional induzida $g' : H' \to S$ com $g = g' \circ f$. Como f leva $H(K_0)$ a $H'(K_0)$, podemos assumir que $\mathrm{Ker}g$ é trivial.

A imagem $g[H]$ contém A, que é denso em S, de modo que $g[H] = S$. Seja h a inversa de g. Então h é quase-racional. Compondo com uma potência da função de Frobenius e alterando H apropriadamente, podemos assumir h racional. QED

Tradicionalmente, um último parágrafo deve ser dedicado a novos horizontes. A existência deles, nesta expedição de Hrushovski, é excepcionalmente nítida. Em Geometria Algébrica, Teoria dos Modelos "interna" ou qualquer outro ramo da Matemática, as ferramentas que apresentamos têm aplicação crescente. Não a explicitaremos, porém: convidamos o leitor a buscá-la ou criá-la em qualquer tópico que lhe chame a atenção.

Referências

[Bouscaren A] E. Bouscaren, *Introduction to model theory*, in [MTAG], p. 1–18.

[Bouscaren B] E. Bouscaren, *Proof of the Mordell–Lang conjecture for function fields*, in [MTAG], p. 177–196.

[Chang, Keisler] C. C. Chang, H. J. Keisler, *Model Theory*, 3ª edição, North-Holland Publishing Company, 1990 (reimpresso 1991).

[Hartshorne] R. Hartshorne, *Algebraic Geometry*, 3ª impressão corr., Springer-Verlag, 1983.

[Hindry] M. Hindry, *Introduction to abelian varieties and the Mordell Lang Conjecture*, in [MTAG], p. 85–100.

[Hindry, Silverman] M. Hindry, J. H. Silverman, *Diophantine Geometry: An Introduction*, Springer-Verlag, 2000.

[Hodges] W. Hodges, *Model Theory*, Cambridge University Press, 1993 (reimpresso 1997).

[Hrushovski] E. Hrushovski, *The Mordell–Lang Conjecture for function fields*, Journal AMS, vol. 9, no. 3, 1996, p. 667–690.

[Hrushovski, Zilber] E. Hrushovski, B. Zilber, *Zariski geometries*, Journal AMS, vol. 9, no. 1, 1996, p. 1–56.

[Jacobson I] N. Jacobson, *Basic Algebra I*, 2ª edição, W. H. Freeman and Company, 1985.

[Jacobson II] N. Jacobson, *Basic Algebra II*, 1ª edição, W. H. Freeman and Company, 1980. (Existe a 2ª edição, de 1989.)

[Lang] S. Lang, *Algebra*, 3ª edição revisada, Springer-Verlag, 2002.

[Lang 1] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, 1983.

[Lang 2] S. Lang, *Number Theory III: Diophantine Geometry*, Springer-Verlag, 1991.

[Lascar] D. Lascar, *Omega-stable groups*, in [MTAG], p. 45–59.

[Marker] D. Marker, *Model Theory: An Introduction*, Springer-Verlag, 2002.

[Marker A] D. Marker, *Zariski geometries*, in [MTAG], p. 107–128.

[MTAG] E. Bouscaren (ed.), *Model Theory and Algebraic Geometry: An introduction to E. Hrushovski's proof of the geometric Mordell–Lang conjecture*, 2ª impressão corrigida, LNM 1696, Springer-Verlag, 1999.

[Pillay] A. Pillay, *Geometric Stability Theory*, Oxford University Press, 1996.

[Pillay 97] A. Pillay, *Model Theory and Diophantine Geometry*, Bulletin AMS (NS), vol. 34, no. 4, 1997, p. 405–422. Com correção no vol. 35, no. 1, 1998, p. 67.

[Pillay A] A. Pillay, *Model theory of algebraically closed fields*, in [MTAG], p. 61–84.

[Pillay B] A. Pillay, *The model-theoretic content of Lang's conjecture*, in [MTAG], p. 101–106.

[Poizat 1] B. Poizat, *A Course in Model Theory*, Springer-Verlag, 2000. (Tradução de M. Klein do original em francês *Cours de Théorie des modèles*, Nur al-Mantiq wal-Ma'rifah, 1985.)

[Poizat 2] B. Poizat, *Stable Groups*, American Mathematical Society, 2001. (Tradução de M. Klein do original em francês *Groupes Stables*, Nur al-Mantiq wal-Ma'rifah, 1987.)

[Shafarevich] I. R. Shafarevich, *Basic Algebraic Geometry*, Springer-Verlag, 1977.

[Shelah] S. Shelah, *Classification Theory and the Number of Non-Isomorphic Models*, edição revisada, North-Holland Publishing Company, 1990.

[Ziegler] M. Ziegler, *Introduction to stability theory and Morley rank*, in [MTAG], p. 19–44.

Índice